

(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局(43) 国際公開日
2003 年 11 月 6 日 (06.11.2003)

PCT

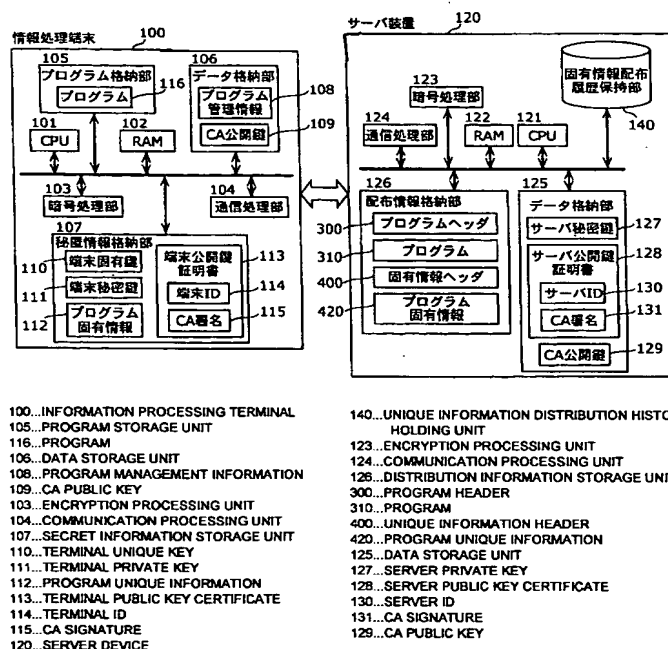
(10) 国際公開番号
WO 03/091862 A1

- (51) 国際特許分類: G06F 1/00, 9/445 (72) 発明者; および
(75) 発明者/出願人 (米国についてののみ): 前田 卓治 (MAEDA, Takuji) [JP/JP]; 〒572-0052 大阪府 寝屋川市 上神田 2 丁目 20 番 1-501 号 Osaka (JP). 三浦 康史 (MIURA, Kouji) [JP/JP]; 〒580-0016 大阪府 松原市 上田 3 丁目 4 番 1 号 Osaka (JP). 徳田 克己 (TOKUDA, Katsumi) [JP/JP]; 〒563-0038 大阪府 池田市 荘園 1 丁目 13 番 2 号 Osaka (JP). 井上 信治 (INOUE, Shinji) [JP/JP]; 〒572-0081 大阪府 寝屋川市 東香里園町 9 番 13-306 号 Osaka (JP).
- (21) 国際出願番号: PCT/JP03/04808
- (22) 国際出願日: 2003 年 4 月 16 日 (16.04.2003)
- (25) 国際出願の言語: 日本語
- (26) 国際公開の言語: 日本語
- (30) 優先権データ:
特願2002-120430 2002 年 4 月 23 日 (23.04.2002) JP
- (71) 出願人 (米国を除く全ての指定国について): 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.) [JP/JP]; 〒571-8501 大阪府 門真市 大字門真 1006 番地 Osaka (JP).
- (74) 代理人: 新居 広守 (NIJ, Hiromori); 〒532-0011 大阪府 大阪市淀川区 西中島 3 丁目 11 番 26 号 新大阪末広センタービル 3F 新居国際特許事務所 Osaka (JP).
- (81) 指定国 (国内): CN, KR, US.
- (84) 指定国 (広域): ヨーロッパ特許 (DE, GB).

[続葉有]

(54) Title: SERVER DEVICE AND PROGRAM MANAGEMENT SYSTEM

(54) 発明の名称: サーバ装置及びプログラム管理システム



(57) Abstract: A server device (120) comprises a CPU (121); a RAM (122); an encryption processing unit (123) that performs encryption and decryption processing; a communication processing unit (124) that performs communication with an information processing terminal (100); a data storage unit (125) in which information that need not be kept secret is stored; a distribution information storage unit (126) in which information on a program to be distributed and so on is stored; and a unique information distribution history holding unit (140) that holds a unique information distribution history (600) used to manage the history of program unique information on a program previously distributed to the information processing terminal (100).

[続葉有]



添付公開書類:

- 国際調査報告書
- 補正書・説明書

2文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約:

サーバ装置(120)は、CPU(121)、RAM(122)、暗号化及び復号化処理を行う暗号処理部(123)、情報処理端末(100)との通信を行う通信処理部(124)、秘匿する必要がない情報を格納するデータ格納部(125)、配布するプログラムなどの情報を格納する配布情報格納部(126)、及び情報処理端末(100)に以前に配布したプログラムのプログラム固有情報の履歴を管理するための固有情報配布履歴(600)を保持する固有情報配布履歴保持部(140)を有する。

明 細 書

サーバ装置及びプログラム管理システム

5 技術分野

本発明は、情報処理端末で動作するプログラムの配布を行うサーバ装置、及びサーバ装置と情報処理端末からなるプログラム管理システムに関し、特に不正なプログラムの使用を図る情報処理端末の排除における技術に関する。

10

背景技術

近年のネットワークの発展に伴い、ネットワークを経由して商取引を行う電子商取引システム（Electronic commerce system）、映画、音楽等のコンテンツの配信を行うコンテンツ配信システムが多く発表されている。これらのシステムにおいては、ネットワークを介して接続される機器間で、コンテンツの利用権利、課金に使用する鍵等の価値ある情報データのみになく、音楽プレーヤプログラム等のプログラム自体を交換することも可能である。また、このようなプログラムの交換は、従来のPC以外にも携帯電話等の組込み機器においても実現されることが予測される。

20

そして、電子ショッピングやコンテンツ配信サービスなど、課金を伴う商用システムをネットワークを介して実現する場合においては、悪意のあるユーザが不正にプログラムを書き換えることが可能であれば、課金情報の操作により無料で商品やコンテンツを購入するなどの不正行為が行われる危険性がある。そのため、ネットワーク経由のプログラム更新による不具合修正や追加を行う場合、悪意のあるユーザの不正使用を

25

防止するために、プログラムの正当性を検証する必要がある。

従来プログラムの正当性を検証する方法としては、電子的な署名を用いる方法が存在する(例えば、特開 2 0 0 0 - 3 3 9 1 5 3 号公報参照)。この方法では、公開鍵暗号方式と呼ばれる 2 つの対となる鍵の組を用いた暗号化データ交換方式を利用する。図 2 0 は、この電子的な署名を用いたプログラムの正当性検証方法に関する説明図である。

プログラム発行者 2 0 0 0 は、プログラム発行の身元を確認し、保証する第三者機関である認証局 (C A : Certification Authority) 2 0 1 0 に公開鍵 2 0 0 1 を送付する。その後、認証局 2 0 1 0 は、プログラム発行者 2 0 0 0 の身元を確認、審査する。認証局 2 0 1 0 がプログラム発行者 2 0 0 0 を信頼できると判断した場合、プログラム発行者 2 0 0 0 の公開鍵 2 0 0 1 に対し C A 秘密鍵 2 0 1 2 で電子的な署名を行った証明書 2 0 0 3 を発行する。証明書 2 0 0 3 は公開鍵保有者の身元を識別する情報を含み、認証局 2 0 1 0 が公開鍵保有者の身元を保証するものである。そして、認証局 2 0 1 0 は、プログラム発行者 2 0 0 0 に公開鍵証明書 2 0 0 3 を送付する。

プログラム発行者 2 0 0 0 は、ユーザ 2 0 2 0 に配布するプログラムに対し、自己の秘密鍵 2 0 0 2 で電子的な署名を行い、公開鍵証明書 2 0 0 3、及び署名付きプログラム 2 0 0 4 を配布する。

ユーザ 2 0 2 0 は、認証局 2 0 1 0 から C A 公開鍵 2 0 1 1 を取得し、C A 公開鍵 2 0 1 1 を用いてプログラム発行者の公開鍵証明書 2 0 0 3 の署名を検証する。署名の検証が正しく行われた場合、公開鍵証明書 2 0 0 3 に含まれる公開鍵 2 0 0 1 を用いて署名付きプログラム 2 0 0 4 の署名を検証する。この署名の検証が正しく行われた場合、配布されたプログラムがプログラム発行者 2 0 0 0 から配布されたプログラムであり、改ざんされていないことを検証できる。

従って、この正当性検証方式においては、プログラムにプログラム発行者 2000 の電子的な署名を付加することによりプログラムの正当性を保証して、ユーザ 2020 は取得したプログラム 2021 がプログラム発行者 2000 から正当に配布されたものであることを検証できる。

5 しかし、図 20 に示す正当性検証方式においては、配布時におけるプログラムの正当性検証は行えるが、配布後の情報処理端末におけるプログラムに関して正当性を保証することはできない。尚、公開鍵暗号方式及び証明書、署名、認証の仕組みに関しては、種々の文献（例えば、「Applied Cryptography」Bruce Schneier, John Wiley & Sons, Inc (1996) 参照）
10 に詳細が記されている。

この問題点を解決する方法として、プログラム配布先のユーザ識別子を用いてプログラム配布元でプログラムを暗号化して配布し、ユーザは使用時にユーザ識別子を用いてプログラムを復号化して実行する方法がある（例えば、特開平 7-295800 号公報参照）。この方法では、
15 万が一プログラムが不正にコピーされたとしても、ユーザ識別子が一致しなければプログラムを復号し実行することができないため、不正コピー、不正改ざんを防止することが可能となる。

また、プログラムの配布装置としては、プログラムの配布に当たって
20 配布の妥当性をプログラムのコピー数とコピー許可数の差により判定して、無制限な配布が行われることを物理的に防ぐことができ、プログラムコピーに関する使用契約を物理的に遵守させる配布装置が開示されている（例えば、特公平 6-87220 号公報参照）。

この発明においては、プログラム配布装置は、プログラム毎に情報処理装置の配布先を記憶して、コピー許可数とコピー数とによりプログラムを配布するプログラム配布装置とすることが可能となる。
25

一方、ネットワークを用いた電子ショッピングやコンテンツ配信サービス等の課金を伴う商用システムを実現する場合、ユーザに対する課金を行うため、ユーザを特定する方法が必要となる。この方法の１つとして、プログラムあるいはプログラムと共に配布する情報の中に、ユーザ毎に割り当てるＩＤや鍵などの固有情報を含ませる場合がある。この場合、ユーザ毎に固有情報を割り当て、プログラム配布元のサーバ装置側において固有情報を管理することで、ユーザが不正行為を行った際において固有情報を元にユーザを特定することが可能となる。

図２１は、従来の情報処理端末２１０１とサーバ装置２１０２及び２１０３との間のプログラム管理システムの参考図である。尚、図２１においては説明のためにアプリケーションデータ用のサーバ装置２１０３及びプログラム用のサーバ装置２１０２に分けて示す。

情報処理端末２１０１は、プログラム配布元となるサーバ装置２１０２から、例えば好みの音楽データをダウンロードして再生可能な音楽プレーヤプログラムを取得する。この音楽プレーヤプログラムには固有情報「０１０１」が含まれるとする。尚、プログラムの安全な配布を図るために、通信路はＳＳＬ（Secure Socket Layer）を用いて暗号化し、盗聴等のハッキング行為を防止する。

情報処理端末２１０１の利用者が音楽データ等の取得を要求する際においては、情報処理端末２１０１から前記固有情報「０１０１」が付与された音楽データ取得要求をアプリケーション用のサーバ装置２１０３に送信する。そして、サーバ装置２１０３は、不正な音楽プレーヤプログラムが実行される情報処理端末を排除するための無効化リスト（ＣＲＬ：certificate revocation list）を有しており、情報処理端末２１０１から音楽データ取得要求に合わせて送信される固有情報「０１０１」がＣＲＬに記載されているため情報処理端末２１０１に音楽データの送

信を行わない。尚、CRLに固有情報が記載されていない場合においては要求される音楽データを情報処理端末2101に送る。

このように、不正なプログラム使用を行っている情報処理端末2101の有するプログラムの固有情報を特定すれば、CRLを用いて不正使用を図る情報処理端末2101を排除することが可能となる。

尚、サーバ装置2102等から情報処理端末2101にダウンロードされるデータに電子的な署名を付加して、情報処理端末2101側で署名検証を行うことにより、ダウンロードデータの改ざん、すり替え、盗聴等を防止して、不正行為からダウンロードデータを守る安全な配布も可能となる。

しかしながら、上述したプログラム配布元において各ユーザ識別子に応じたプログラム暗号処理を行う方法においては、プログラム配布元にかかる処理の負担が大きくなるという問題が生じる。

また、上述したプログラム配布装置がプログラム毎に情報処理装置の配布先を記憶して、コピー許可数とコピー数とによりプログラムを配布する方法は、プログラム配布装置はプログラムの配布要求毎に配布先の装置のIDを確認してコピー許可数に従ってプログラムを配布するものであり、プログラムの不正使用を防止するものではない。

さらに、図21に示すサーバ装置2103がプログラムの固有情報を記載したCRLを用いて不正利用を図る情報処理端末2101の排除を行う方法においては、情報処理端末2101が不正にデータを取得しようと試み、サーバ装置2103のCRLにより不正端末としてデータ取得を排除される場合においても、情報処理端末2101の使用者が、別の固有情報のダウンロードをサーバ装置2102から行いプログラムの固有情報を新たな固有情報に更新することによりサーバ装置2103のCRLを用いた排除から回避することが可能となるという問題がある。

本発明は以上のような課題に鑑みてなされたものであり、プログラム配布元であるサーバ装置において、固有情報を用いたリストにより排除された不正な情報処理端末が新規な固有情報を取得して排除を回避することを防止するサーバ装置を提供することを第１の目的とする。また、

5 情報処理端末へのプログラム配信においてサーバ装置の処理負担を少なくすることを目的とする。

そして、サーバ装置と情報処理端末との間においてプログラムの配布を行うプログラム管理システムにおいても、不正な情報処理端末からの新規な固有情報の取得要求を排除して情報処理端末でのプログラムの不正使用を防ぐことが可能なプログラム管理システムを提供することを目的とする。

10

発明の開示

前記課題を解決するために、本発明に係るサーバ装置は、外部から書き換えが行えない端末ＩＤを保持する情報処理端末とネットワークを介して接続され前記情報処理端末で動作するプログラムを保持するサーバ装置であって、以前に配布したプログラムと端末ＩＤとの関連を示すテーブルを保持するテーブル保持手段と、前記テーブルを参照して、前記情報処理端末から送信され前記端末ＩＤを伴うプログラム取得要求に対するプログラムの配布の可否を判定する判定手段とを備えることを特徴とする。

15

20

また、本発明に係るサーバ装置から情報処理端末に配布されるプログラムには、前記情報処理端末で動作するプログラム本体及び前記プログラム本体に使用される固有の情報であるプログラム固有情報が含まれ、

25 前記判定手段は、前記プログラム取得要求に付与されている前記端末ＩＤが前記テーブルに記録されている場合には、前記プログラム固有情報

の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、前記端末IDが前記テーブルに記載されていない場合には、前記端末IDと前記プログラム固有情報とを対応させて前記テーブルに追加すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定することを特徴とする。

これらにより、サーバ装置は、情報処理端末が以前に配布したプログラムに対応するプログラム固有情報の新規取得を防止することが可能となり、新たなプログラム固有情報を取得して排除の回避を図る情報処理端末の不正行為を確実に防止することが可能となる。

そして、前記課題を解決するために、本発明に係るプログラム管理システムは、外部から書き換えが行えない端末IDを保持する情報処理端末と、当該情報処理端末とネットワークを介して接続され前記情報処理端末で動作するプログラムを保持するサーバ装置とから構成されるプログラム管理システムであって、前記情報処理端末は、前記プログラムの取得を要求する場合には、前記端末IDを付与したプログラム取得要求を前記サーバ装置に送信し、前記サーバ装置は、前記プログラム取得要求を受信して、以前に配布したプログラムと端末IDとの関連を示すテーブルを保持するテーブル保持手段と、前記テーブルを参照して、前記情報処理端末から送信されて前記端末IDが付与されているプログラム取得要求に対するプログラムの配布の可否を判定する判定手段とを備えることを特徴とする。

このように、本発明は、上述のようなサーバ装置として実現できるのみではなく、サーバ装置と情報処理端末との間のプログラム管理システムやサーバ装置が備える手段をステップとするプログラム配布方法としても実現できる。また、このプログラム配布方法をコンピュータ等で実現させるプログラムとして実現したり、当該プログラムをCD-ROM

等の記録媒体や通信ネットワーク等の伝送媒体を介して流通させることができるのは言うまでもない。

図面の簡単な説明

5 図 1 は、実施の形態 1 における情報処理端末とサーバ装置との構成図を示している。

図 2 は、本実施の形態 1 に係るサーバ装置から情報処理端末側に送信されるプログラム全体の構成図である。

10 図 3 (a) は、プログラムヘッダに格納される情報の一例を示す図である。

図 3 (b) は、プログラムに格納される情報の一例を示す図である。

図 4 (a) は、固有情報ヘッダに格納される情報の一例を示す図である。

15 図 4 (b) は、プログラム固有情報に格納される情報の一例を示す図である。

図 5 は、情報処理端末とサーバ装置と間で行われるプログラム更新システムにおける動作手順を示す図である。

図 6 は、固有情報配布履歴保持部に保持される固有情報配布履歴の情報格納の一例を示す図である。

20 図 7 は、サーバ装置におけるプログラムの配布手順を示すフローチャートである。

図 8 は、本実施の形態 1 に係るサーバ装置を用いたプログラム管理システムを示す全体図である。

25 図 9 は、本実施の形態 1 に係るプログラムヘッダとプログラムに含まれる別のデータ構造を示す図である。

図 10 は、固有情報ヘッダとプログラム固有情報とに含まれる別のデ

一タ構造を示す図である。

図 1 1 は、本発明の実施の形態 2 に係る情報処理端末とサーバ装置との構成図を示す。

図 1 2 (a) は、本実施の形態 2 に係る固有情報配布履歴に含まれる
5 情報の一例を示す図である。

図 1 2 (b) は、本実施の形態 2 に係るプログラム／固有情報対応表に含まれる情報の一例を示す図である。

図 1 3 は、サーバ装置におけるプログラムの配布手順を示すフローチャートである。

10 図 1 4 は、本実施の形態 3 に係る情報処理端末とサーバ装置の構成図を示す。

図 1 5 は、本実施の形態 3 に係る配布回数情報の情報格納例を示す図である。

図 1 6 は、サーバ装置におけるプログラムの配布手順を示すフローチャートである。
15

図 1 7 は、本実施の形態 4 に係る情報処理端末とサーバ装置の構成図を示す。

図 1 8 (a) は、本実施の形態 4 に係る配布回数情報に格納されるデータの一例を示す図である。

20 図 1 8 (b) は、本実施の形態 4 に係るプログラム／固有情報対応表に格納されるデータの一例を示す図である。

図 1 9 は、サーバ装置におけるプログラムの配布手順を示すフローチャートである。

図 2 0 は、従来の電子的な署名を用いたプログラムの正当性検証方法
25 に関する説明図である。

図 2 1 は、従来の情報処理端末とサーバ装置との間のプログラム管理

システムの参考図である。

発明を実施するための最良の形態

以下、本発明の実施の形態に係るサーバ装置及びプログラム管理システムについて図面を用いて説明する。

(実施の形態 1)

図 1 は本発明の実施の形態 1 における情報処理端末 100 とサーバ装置 120 との構成図を示している。

情報処理端末 100 は、サーバ装置 120 から取得した電子商取引やコンテンツ配信等に用いられるプログラムを使用する端末装置であり、CPU 101、RAM 102、プログラムやデータ等の暗号化及び復号化処理を行う暗号処理部 103、サーバ装置 120 との通信を行う通信処理部 104、プログラムを格納するプログラム格納部 105、CA 公開鍵など特に秘匿する必要がない情報を格納するデータ格納部 106、及び秘密鍵など秘匿する必要がある情報を格納する秘匿情報格納部 107 から構成されている。

プログラム格納部 105 は、CPU 101 で動作するプログラム 116 を格納する。

データ格納部 106 は、情報処理端末 100 で使用されるデータのうち特に秘匿する必要がないものを格納すると共に、情報処理端末 100 に格納されているプログラムの ID やバージョン番号など格納プログラムの管理情報であるプログラム管理情報 108 及び CA 公開鍵 109 を格納する。

また、秘匿情報格納部 107 は、情報処理端末 100 内で秘匿する必要がある情報を格納しており、情報処理端末毎に異なる鍵である端末固有鍵 110、情報処理端末毎に異なる公開鍵ペアの 1 つである端末秘密

鍵 1 1 1、プログラムが使用する固有鍵などのプログラム固有情報 1 1
2、情報処理端末毎に異なる公開鍵ペアの他方である端末公開鍵証明書
1 1 3 を格納する。そして、端末公開鍵証明書 1 1 3 は情報処理端末 1
0 0 を一意に識別する ID である端末 ID 1 1 4、端末公開鍵証明書 1
5 1 3 に対し認証局が付加した CA 署名 1 1 5 を含んでいる。

一方、本発明に係るサーバ装置 1 2 0 は、情報処理端末 1 0 0 から要
求されるプログラムを配布する装置であり、CPU 1 2 1、RAM 1 2
2、プログラムやデータなどの暗号化及び復号化処理を行う暗号処理部
1 2 3、情報処理端末 1 0 0 との通信を行う通信処理部 1 2 4、CA 公
10 開鍵など特に秘匿する必要がない情報を格納するデータ格納部 1 2 5、
情報処理端末 1 0 0 に配布するプログラムなどの情報を格納する配布情
報格納部 1 2 6、及び固有情報配布履歴保持部 1 4 0 とから構成されて
いる。

そして、本発明に係るサーバ装置 1 2 0 は、固有情報配布履歴保持部
15 1 4 0 を有することを特徴としている。この固有情報配布履歴保持部 1
4 0 は、情報処理端末 1 0 0 に配布したプログラムのプログラム固有情
報の履歴を管理するための固有情報配布履歴 6 0 0 を保持している。

データ格納部 1 2 5 は、サーバ装置 1 2 0 が使用する情報を格納する
領域であり、公開鍵ペアの 1 つであるサーバ秘密鍵 1 2 7、公開鍵ペア
20 の他方であるサーバ公開鍵証明書 1 2 8、及び CA 公開鍵 1 2 9 を格納
する。サーバ公開鍵証明書 1 2 8 は、サーバを一意に識別する ID であ
るサーバ ID 1 3 0、サーバ公開鍵証明書に対し CA が付加した CA 署
名 1 3 1 を含んでいる。配布情報格納部 1 2 6 は、サーバ装置 1 2 0 が
情報処理端末 1 0 0 に対して配布する情報を格納する領域であり、プロ
25 グラムヘッダ 3 0 0、プログラム 3 1 0、固有情報ヘッダ 4 0 0、及び
プログラム固有情報 4 2 0 を格納する。尚、この配布情報であるプログ

ラム全体の図は後述の図 2 に示す。

配布情報格納部 126 に格納されているプログラムヘッダ 300、プログラム 310、固有情報ヘッダ 400、及びプログラム固有情報 420 には第三者認証機関である CA 署名が付加されており、この CA 署名により配布情報が正当な配布元から配布されるものであることを保証する。

図 2 は、本実施の形態 1 に係るサーバ装置 120 から情報処理端末 100 側に送信されるプログラム全体 200 の構成図である。このプログラムの全体 200 はサーバ装置 120 の配布情報格納部 126 に格納される情報であり、本実施の形態 1 においては、プログラムヘッダ 300、プログラム 310、固有情報ヘッダ 400 及びプログラム固有情報 420 より構成される。また、本発明においては、プログラム全体 200 をプログラム 310 及びプログラム固有情報 420 に分離し、さらに、ヘッダ部とデータ部とに分離することを特徴としている。

尚、本実施の形態に係るプログラム管理システムにおいては、情報処理端末 100 がプログラム 310 で使用するアプリケーションデータをサーバ装置 120 等から取得する場合においては、アプリケーションデータ取得要求にプログラム固有情報 420 を付与して送信する。このことにより、サーバ装置 120 等が有するプログラム固有情報 420 を用いた CRL により不正な情報処理端末を排除することが可能となる。

図 3 (a) 及び (b) は、プログラムヘッダ 300 及びプログラム 310 に格納される情報の一例を示す図である。

プログラムヘッダ 300 は、プログラム 310 に関する情報を格納するものであり、次の情報を含む。

(1) プログラムヘッダ 300 が格納する情報がどのプログラム 310 に対応する情報かを示すプログラム ID (301)。(2) 対応する

プログラム 310 のバージョン番号 (302)。(3) 対応するプログラム 310 のプログラムサイズ (303)。(4) 対応するプログラム 310 のハッシュ値 (304)。(5) 前記 (1) から (4) までの情報を含むプログラムヘッダ 300 全体に対する CA 署名 (305)。

- 5 また、プログラム 310 には、プログラム 310 に対する CA 署名 (311) が付加されている。このように、プログラムヘッダ 300 及びプログラム 310 は共に CA 署名 305 及び 311 を含むため、情報処理端末 100 においてプログラムヘッダ、プログラムが正当な配布元から配布されたものであることを検証することが可能である。

- 10 図 4 (a) 及び (b) は、固有情報ヘッダ 400 及びプログラム固有情報 420 に格納される情報の一例を示す図である。

固有情報ヘッダ 400 は、プログラム固有情報 420 に関する情報を格納するものであり、次の情報を含む。

- 15 (1) 固有情報ヘッダ 400 が格納する情報がどのプログラム固有情報 420 に対応した情報かを示すプログラム固有情報 ID (401)。

- 20 (2) 対応するプログラム固有情報 420 を使用するプログラム 310 のプログラム ID (402)。(3) 対応するプログラム固有情報 420 が格納する固有情報の数 (403)。(4) 対応するプログラム固有情報 420 全体のサイズ (404)。(5) 対応するプログラム固有情報 420 に含まれる個々の固有情報に関する情報示す固有情報サブヘッダ (405)。固有情報サブヘッダ 405 はプログラム固有情報 420 に含まれる個々の固有情報の数 (1 ~ n) だけ存在する。(6) 前記 (1) から (5) までの情報を含む固有情報ヘッダ 400 全体に対する CA 署名 (406)。

- 25 固有情報サブヘッダ 405 は、さらに個々の固有情報を識別するための ID であるプログラム固有情報サブ ID 411、個々の固有情報のサ

イズ 4 1 2 から構成される。

また、プログラム固有情報 4 2 0 は、複数のプログラム固有情報（4 2 1）と、プログラム固有情報全体に対する CA 署名（4 2 2）を含む。このため、固有情報ヘッダ 4 0 0、プログラム固有情報 4 2 0 は共に C
5 A 署名（4 0 6 及び 4 2 2）を含むため、情報処理端末 1 0 0 において固有情報ヘッダ 4 0 0、プログラム固有情報 4 2 0 が正当な配布元から配布されたものであることを検証することが可能である。

次に情報処理端末 1 0 0 とサーバ装置 1 2 0 との間で行われるプログラム更新システムにおける動作手順の例を、図 5 を用いて説明する。こ
10 のプログラム更新システムにおいて、情報処理端末 1 0 0 は、まず、ヘッダ取得要求を行い、空き領域の確認を行う。また、サーバ装置 1 2 0 においては、固有情報配布履歴保持部 1 4 0 から固有情報配布履歴 6 0 0 を参照することにより、プログラムの不正使用を図る情報処理端末 1 0 0 を排除することが可能となる。

15 最初に、情報処理端末 1 0 0 はサーバ装置 1 2 0 と SSL による接続を行う（S 5 0 1）。この際、サーバ装置 1 2 0 は情報処理端末 1 0 0 の端末 ID の取得を行う。尚、SSL は、2 点間でデータを安全に送受信するために、公開鍵暗号方式と秘密鍵暗号方式を併用して、データを暗号化して送受信する仕組みである。また、SSL ではセッション鍵と
20 呼ばれるそのセッションでのみ有効な鍵を共有するため、図 5 に示す S 5 0 2 以降の情報処理端末 1 0 0 とサーバ装置 1 2 0 間のデータ送受信は、すべてセッション鍵を用いた暗号化データにより行われるものとする。

次に、情報処理端末 1 0 0 はサーバ装置 1 2 0 に対し、取得したいプ
25 ログラム 3 1 0 のプログラム ID を指定してヘッダ取得要求を行う（S 5 0 2）。この際、サーバ装置 1 2 0 は、固有情報配布履歴保持部 1 4

0に保持されている固有情報配布履歴600により、端末IDとプログラム固有情報IDとの対応関係を確認する。つまり、情報処理端末100に対して、固有情報IDを既に配布したかどうかを確認する。そして、正規の情報処理端末からのヘッダ取得要求であると判断する場合においては、ヘッダ取得要求を受信したサーバ装置120は、配布情報格納部126に格納したプログラムヘッダ300を情報処理端末100に送信する（S503）。

そして、サーバ装置120からプログラムヘッダ300を受信した情報処理端末100は、データ格納部106に格納しているCA公開鍵109を用いて、プログラムヘッダ300に含まれているCA署名を検証する（S504）。これにより、情報処理端末100はプログラムヘッダ300が改ざんされていない正当な配布元から配布された情報であることを検証する。また、プログラムヘッダ300には、プログラムのプログラムID301、バージョン番号302、サイズ303、プログラムのハッシュ値304などプログラムに関する情報が格納されているため、情報処理端末100は、これらの情報と、データ格納部106に格納されているプログラム管理情報108内に記載されているプログラムID、バージョン情報、空き容量情報を比較し、更新対象のプログラム310が正しくサーバ装置120から配布されたか、プログラム310を格納する空き容量が存在するか確認する（S504）。このため、本実施の形態1に係る情報処理端末100はプログラム310のダウンロード中にプログラムの取得不可となるような弊害を防止する。

次に、サーバ装置120は配布情報格納部126に格納した固有情報ヘッダ400を情報処理端末100に送信する（S505）。

そして、サーバ装置120から固有情報ヘッダ400を受信した情報処理端末100は、データ格納部106に格納しているCA公開鍵10

9を用いて、固有情報ヘッダ400に含まれているCA署名を検証する(S506)。これにより、情報処理端末100は固有情報ヘッダ400が改ざんされていない、正当な配布元から配布された情報であることを検証する。固有情報ヘッダ400には、プログラム固有情報420を一意に識別するプログラム固有情報ID401、プログラム固有情報に関連するプログラムのプログラムID402、プログラム固有情報で配布される情報に含まれる固有情報の数403、サイズ404などプログラム固有情報420に関する情報が格納されているため、情報処理端末100は、これらの情報と、データ格納部106に格納されているプログラム管理情報108内に記載されているプログラムID、空き容量情報を比較し、更新対象のプログラム310に関するプログラム固有情報420が正しくサーバ装置120から配布されたか、プログラム固有情報420を格納する空き容量が存在するかプログラム310のダウンロードの前に確認する(S506)。

15 そして、情報処理端末100は、プログラム310、プログラム固有情報420の取得が行えると判断した場合、サーバ装置120に対しプログラムIDを指定してプログラム取得要求を行う(S507)。

20 そして、プログラム取得要求を受信したサーバ装置120は、配布情報格納部126に格納したプログラム310を情報処理端末100に送信する(S508)。サーバ装置120からプログラム310を受信した情報処理端末100は、データ格納部106に格納しているCA公開鍵109を用いて、プログラム310に含まれているCA署名を検証する(S509)。これにより、情報処理端末100はプログラム310が改ざんされていない、正当な配布元から配布された情報であることを
25 検証する。取得データの正当性が検証できた場合、取得したプログラム310を秘匿情報格納部107に格納している端末固有鍵110で暗号

化し、プログラム格納部 105 に格納する (S509)。その際、プログラム格納位置やプログラム ID、バージョン番号などをプログラム管理情報 108 に格納し、プログラムの管理を行う。

次に、プログラムの格納が完了した後、プログラム格納部 105 に格納したプログラム 116 を、端末固有鍵 110 を用いて復号し、ハッシュ値を算出する。算出した値とプログラムヘッダ 300 に格納されているハッシュ値の比較を行い、プログラムが正しく格納されていることを確認する (S510)。

次に、情報処理端末 100 はサーバ装置 120 に対しプログラム ID を指定してプログラム固有情報取得要求を行う (S511)。

そして、サーバ装置 120 は配布情報格納部 126 に格納したプログラム固有情報 420 を情報処理端末 100 に送信する (S512)。サーバ装置 120 からプログラム固有情報 420 を受信した情報処理端末 100 は、データ格納部 106 に格納している CA 公開鍵 109 を用いて、プログラム固有情報 420 に含まれている CA 署名を検証する (S513)。これにより、情報処理端末 100 はプログラム固有情報が改ざんされていない、正当な配布元から配布された情報であることを検証する。取得データの正当性が検証できた場合、取得したプログラム固有情報を秘匿情報格納部 107 に格納する (S513)。

最後に、情報処理端末 100 におけるプログラム、プログラム固有情報の格納が完了した後、情報処理端末 100 とサーバ装置 120 との間の通信を切断する (S514)。

このように、本実施の形態 1 に係る情報処理端末 100 は、ヘッダ取得要求を行うことによりプログラム 310 を格納する空き容量が存在するか等の確認して、より安全にプログラムのダウンロードを行うことが可能となる。尚、この場合において、プログラム 310 及びプログラム

固有情報 420 のハッシュ値を算出して、算出したハッシュ値と、プログラムヘッダ 300 及びプログラム固有情報ヘッダ 400 に格納されているハッシュ値とを比較することにより正当な配布情報であることを確認することとも考え得る。

- 5 図 6 は、固有情報配布履歴保持部 140 に保持される固有情報配布履歴 600 の情報格納の一例を示す図である。

サーバ装置 120 は、以前に情報処理端末 100 に配布したプログラムに対応するプログラム固有情報 420 と当該情報処理端末 100 の端末 ID とを記録したテーブルを固有情報配布履歴 600 とする。

- 10 そして、サーバ装置 120 は、プログラム固有情報 420 を配布した情報処理端末 100 を識別する ID である端末 ID 601、及び配布したプログラム固有情報 420 を識別する ID であるプログラム固有情報 ID 602 を固有情報配布履歴保持部 140 に格納する。また、必要に応じてプログラム固有情報 420 を最後に配布した日時を示す最終配布
15 日付 603 を固有情報配布履歴 600 に格納する。

- 図 6 においては、サーバ装置 120 は情報処理端末 100 に 5 つのプログラム固有情報 420 を配布済みであり、それぞれの端末 ID 601、プログラム固有情報 ID 602 の組は、(端末 ID, プログラム固有情報 ID) = (0001, 0001)、(0002, 0002)、(00
20 10, 0003)、(0015, 0004)、(0020, 0005) となる。

図 7 は、サーバ装置 120 におけるプログラム 310 の配布手順を示すフローチャートである。

- 最初に、サーバ装置 120 は情報処理端末 100 からプログラム配布
25 要求を受信する (S701)。次に、サーバ装置 120 は、受信したプログラム配布要求に含まれる情報処理端末 100 の端末 ID を取得して

(S702)、固有情報配布履歴600に対して取得した端末IDを検索し(S703)、固有情報配布履歴600に同じ端末IDが格納されているか否かの判定を行う(S704)。

サーバ装置120は、固有情報配布履歴600に同じ端末IDが格納
5 されていた場合には(S704のY)、情報処理端末100には既にプログラム固有情報420を配布済みであるため、プログラム310のみを送信し処理を終了する(S708)。

また、サーバ装置120は、固有情報配布履歴600に同じ端末ID
が格納されていない場合(S704でN)、情報処理端末100に対し
10 ては新たにプログラム固有情報420を割り当てて(S705)、この新たに割り当てたプログラム固有情報420に関し、端末ID601とプログラム固有情報ID602の対応を追加して固有情報配布履歴600を更新する(S706)。そして、サーバ装置120は、プログラム固有情報420を情報処理端末100に送信し、プログラム310を情
15 報処理端末100に送信して処理を終了する(S708)。

このように、サーバ装置120において固有情報配布履歴600を用
いてプログラム固有情報を配布管理することにより、1つの情報処理端
末100へ複数のプログラム固有情報420を配布することを確実に防
止する。これにより、サーバ装置120は、既にCRL等によりプログ
20 ラム固有情報420を用いて不正端末と認識され、排除されている情報処理端末100に対しては、新たなプログラム固有情報420を割り当てることはない。従って、新たなプログラム固有情報420を取得して排除の回避を図る情報処理端末100の不正行為を防止することが可能となる。

25 図8は、本実施の形態1に係るサーバ装置120を用いたプログラム管理システムを示す全体図である。

プログラム用のサーバ装置 120 a は、プログラム取得要求に対応するプログラムを情報処理端末 100 に送信する。サーバ装置 120 b は、情報処理端末 100 で動作するプログラムに用いるアプリケーションを情報処理端末 100 に送信する。尚、図 8 においては、情報処理端末 100 の保持するプログラムのプログラム固有情報を「0101」として、
5 CRL 800 の排除からの回避を図るために新たなプログラム固有情報の不正取得を図る端末として説明を行う。また、プログラムの安全な配布を図るために、通信路は SSL を用いて暗号化通信路としている。

情報処理端末 100 の利用者がアプリケーションデータを要求する際
10 においては、情報処理端末 100 の保持するプログラムのプログラム固有情報「0101」を付与したアプリケーション取得要求をアプリケーションデータ用のサーバ装置 120 b に送信する。

そして、サーバ装置 120 b は、プログラム固有情報を用いた不正プログラムの無効化リスト (CRL) 800 を有しており、情報処理端末
15 100 からの取得要求に付与されるプログラム固有情報「0101」が CRL 800 に記載されているためにアプリケーションデータの送信を行わないことで不正な情報処理端末の排除を行う。尚、CRL にプログラム固有情報が記載されていない場合においては、サーバ装置 120 b は、アプリケーションデータを情報処理端末 100 に送る。また、サーバ装置 120 a 等からダウンロードするデータに CA 署名を付加して、
20 情報処理端末 100 で署名検証を行うことにより、ダウンロードデータの通信路上での改ざん、すり替え、盗聴等を防止する。

プログラム固有情報「0101」が CRL 800 に記載された情報処理端末 100 のユーザは、新たな別のプログラム固有情報を得て CRL
25 による排除を回避するためにプログラム用のサーバ装置 120 a よりプログラム固有情報の取得要求を行う。

このような場合において、本発明に係るサーバ装置 120a は、固有情報配布履歴保持部 140 において、以前に配布したプログラムに関し、情報処理端末 100 の端末 ID「0102」と、プログラム固有情報 ID「0101」とを記録した固有情報配布履歴 600 を有している。

- 5 そして、情報処理端末 100 から、新たなプログラム固有情報取得要求をサーバ装置 120a に対して行う場合には、サーバ装置 120a は、このプログラム固有情報取得要求に付与されている端末 ID「0102」が固有情報配布履歴 600 に記載されているか否か判断して、記載されている場合においては、プログラム固有情報の配布を禁止してプログラム
- 10 ム本体のみの配布を前記情報処理端末 100 に行う。尚、固有情報配布履歴 600 を参照して、プログラム固有情報取得要求に付与されている端末 ID に対応するプログラム固有情報 ID が記載されていない場合においては、端末 ID とプログラム固有情報 ID とを対応させて固有情報配布履歴 600 に追加すると共に、プログラムとプログラム固有情報と
- 15 を情報処理端末 100 に配布する。

- 尚、サーバ装置 120a が情報処理端末 100 に再度配布をしないのは、プログラム固有情報のみであり、プログラムの本体は 2 回以上配布しても構わない。これは、プログラム固有情報が CRL 800 により無効化されているため、プログラム固有情報が更新されない限り、不正使用を図る情報処理端末 100 のユーザが新たなアプリケーションデータ
- 20 を取得することを排除しているためである。

- 図 9 は、本実施の形態 1 に係るプログラムヘッダ 900 とプログラム 910 に含まれる別のデータ構造を示す図である。図 9 において、図 3 と異なる点は、プログラム 910 に CA 署名 311 を付加しない点である。
- 25 る。

プログラムヘッダ 900 は、プログラム 910 に関する情報を格納す

るものであり、上述したプログラムヘッダ 300 と同様の情報であるプログラム ID (901)、バージョン番号 (902)、プログラムサイズ (903)、ハッシュ値 (904)、CA 署名 (905) を含むものである。

- 5 プログラムヘッダ 900 及びプログラム 910 の正当性検証を情報処理端末 100 において行う場合、第 1 に、プログラムヘッダ 900 をサーバ装置 120 から取得し、プログラムヘッダ 900 に付加された CA 署名 905 を検証する。これにより、情報処理端末 100 はプログラムヘッダ 900 が改ざんされていない、正当な配布元から配布された情報
- 10 であることを検証する。

- 次に、プログラム 910 のハッシュ値を算出する。算出したハッシュ値と、プログラムヘッダ 900 に格納されているプログラムのハッシュ値 904 を比較し、一致することを確認する。これにより、情報処理端末 120 はプログラム 910 が改ざんされていない正当な配布元から配布された情報であることを検証することが可能となる。
- 15

- このように、プログラム 910 の正当性検証にプログラムヘッダ 900 に格納されたプログラムのハッシュ値 904 を使用し、プログラムヘッダ 900 にのみ CA 署名 905 を付加することで、プログラム 910 の CA 署名に必要とする情報を低減しながら、プログラムヘッダ 900、
- 20 プログラム 910 に署名を付加する場合と同様に正当性を検証することが可能となる。また、プログラムヘッダ 900 とプログラム 910 の組み合わせが不正に変更された場合、情報処理端末 100 において、プログラムのハッシュ値を算出することにより組み合わせの異常を検出することが可能となる。尚、プログラム 910 の CA 署名を行わないことにより、プログラム 910 を認証局に渡して CA 署名を行う必要がなくな
- 25 る。

次に、図 10 を用いて、固有情報ヘッダ 1000 とプログラム固有情報 1020 とに含まれる別のデータ構造を示す図である。図 10 において、図 4 と異なる点は、固有情報ヘッダ 1000 がプログラム固有情報ハッシュ値 1005 を有し、プログラム固有情報 1020 に CA 署名 45 22 を付加しない点である。

固有情報ヘッダ 1000 は、プログラム固有情報 1020 に関する情報を格納するものであり、上述した固有情報ヘッダ 400 に格納される情報と同様な情報であるプログラム固有情報 ID 1001、プログラム ID 1002、固有情報の数 1003、プログラム固有情報全体のサイズ 1004、プログラム固有情報全体のハッシュ値 1005、固有情報サブヘッダ 1006、及び固有情報ヘッダ全体に対する CA 署名 1007 より構成される。

従って、情報処理端末 100 は、プログラム固有情報 1020 のハッシュ値を算出して、算出したハッシュ値と、固有情報ヘッダ 1000 に格納されているプログラム固有情報のハッシュ値 1005 とを比較して一致することを確認することにより、プログラム固有情報 1020 が改ざんされていない、正当な配布元から配布された情報であることを検証することが可能となる。

以上のように、本実施の形態 1 に係るサーバ装置 120 が固有情報配布履歴保持部 140 を有することにより、サーバ装置 120 は、情報処理端末 100 が以前に配布したプログラムに対応するプログラム固有情報の新規取得を防止することが可能となる。このため、新たなプログラム固有情報 420 を取得して排除の回避を図る情報処理端末 100 のハッキング等の不正行為を回避してセキュアなダウンロードを実現できる。

また、情報処理端末 100 においてサーバ装置 120 から取得したプログラムを内部からのみアクセス可能なセキュアなフラッシュメモリ等

に記録されている端末固有鍵 110 で暗号化することにより、従来のようにサーバ装置においてプログラムを情報処理端末の固有の鍵で暗号化する処理を必要としなくなり、サーバ装置 120 におけるプログラム暗号化処理の負担を軽減することが可能となる。尚、この場合、情報処理
5 端末 100 において端末固有鍵 110 で暗号化した場合、正しく暗号化が行えたことを確認する必要がある。この点に関し本発明では、情報処理端末 100 は、プログラム格納後に端末固有鍵 110 で復号し、平文プログラムのハッシュ値による検証を行うことで、情報処理端末 100 毎に異なる端末固有鍵 110 による暗号化を意識することなく、プログラ
10 ム格納の成否を判定することが可能となる。

さらに、サーバ装置 120 は、プログラム全体をプログラム 310 及びプログラム固有情報 420 に分離して個別に作成している。従って、サーバ装置 120 は、各情報処理端末 100 で異なる情報となる容量の比較的小さなプログラム固有情報 420 を複数管理して、全情報処理端
15 末 100 で共通な情報となる容量の大きなプログラム 310 は 1 つのみ管理することにより、サーバ装置 120 で管理する配布情報の容量を格段に低減され、ひいては、情報管理の負担を軽減することが可能となる。

そして、サーバ装置 120 においては、固有情報ヘッダ 1000 にプログラム固有情報 1020 のハッシュ値 1005 を格納し、固有情報ヘッダ 1000 にのみ CA 署名 1007 を付加することで、プログラム 9
20 10 の CA 署名に必要とする情報を低減しながら、固有情報ヘッダ 1000、プログラム固有情報 1020 に署名を付加する場合と同様の効果を得ることが可能となる。また、固有情報ヘッダ 1000 とプログラム固有情報 1020 の組み合わせが不正に変更された場合、情報処理端末
25 100 において、プログラム固有情報 1020 のハッシュ値を算出することにより組み合わせの異常を検出することが可能となる。

尚、本実施の形態 1 で示した固有情報配布履歴保持部 140 に保持される固有情報配布履歴 600 の形式は一例であり、最終配布日付 603 を削除してもよいし、他の情報を付加してもよい。また、本実施の形態 1 では固有情報配布履歴 600 に記載されている端末 ID 601 に対して
5 プログラム固有情報 420 の配布を拒否しているが、不正取得でない限りにおいては、当該端末 ID 601 を有する情報処理端末 100 に対して既に配布済みのプログラム固有情報 420 を再度配布してもよい。

そして、本実施の形態 1 に係るサーバ装置 120 では、情報処理端末 100 からの要求はプログラムの配布を伴うプログラム配布要求、又は
10 プログラムの配布を伴わないプログラム固有情報配布要求のいずれかとなることができる。

また、本実施の形態 1 では情報処理端末 100 とサーバ装置 120 間で SSL を用いた暗号化データの送受信を行っているが、2 点間で安全にデータの送受信が行える方法であれば、SSL に限らず他のプロトコルを用いてもよい。
15

そして、本実施の形態 1 ではデータ格納部 106 とプログラム格納部 105 を別にしているが、同一の格納部としてもよい。また、秘匿情報格納部 107 に端末公開鍵証明書 113 を格納しているが、データ格納部 106 に格納してもよい。

また、本実施の形態 1 に係るサーバ装置 120 は、プログラムヘッダ 300、固有情報ヘッダ 400 をプログラム 310、プログラム固有情報 420 とは別に作成しているが、プログラム 310 とプログラムヘッダ 300、プログラム固有情報 420 と固有情報ヘッダ 400 をそれぞれ一体の情報とし、サーバ装置 120 からの配布に先立ちヘッダ部分のみ切り出して情報処理端末 100 に送信してもよい。
20
25

さらに、本実施の形態 1 ではプログラム 310、プログラム固有情報

420に対し配布時にセッション鍵による暗号化を行う例を示したが、セッション鍵とは異なる鍵でさらに暗号化し、その鍵をプログラムヘッダ300、固有情報ヘッダ400に含めて配布する構成としてもよい。

そして、本実施の形態1でハッシュ値と記載している点は、ハッシュ
5 アルゴリズムとしてSHA-1、MD5などの既存のハッシュアルゴリズムを使用してもよいし、独自のアルゴリズムを用いてもよい。また、ハッシュアルゴリズムのかわりにチェックサムなどの方法を用いて改ざんの検出を行ってもよい。また、情報処理端末100毎に異なる情報を必要としないプログラムを配布する場合は、プログラム固有情報の配布
10 を行う必要はない。

(実施の形態2)

図11は、本発明の実施の形態2に係る情報処理端末1100とサーバ装置1120との構成図を示す。同図において、実施の形態1と異なる点は、サーバ装置1120がプログラム／固有情報対応表保持部11
15 50を保持する点である。

このプログラム／固有情報対応表保持部1150は、プログラム固有情報を一意に識別するプログラム固有情報IDと、プログラム固有情報を使用するプログラムを一意に特定するプログラムIDとの対応を示したプログラム／固有情報対応表1210を保持する記憶部である。

20 図12(a)及び(b)は、本実施の形態2に係る固有情報配布履歴1200及びプログラム／固有情報対応表1210に含まれる情報の一例を示す図である。

固有情報配布履歴保持部1140は、前述した実施の形態1の固有情報配布履歴600と異なり、配布したプログラム固有情報に対応するプ
25 ログラムを識別するプログラムID1202が付加されている固有情報配布履歴1200を管理する。尚、固有情報配布履歴1200に格納さ

れる端末ID1201、プログラム固有情報ID1203、及び最終配布日付1204については前述した図6と同様のため詳細な説明は省略する。

固有情報配布履歴1200の例では、サーバ装置1120は情報処理
5 端末1100に5つのプログラム固有情報ID1203を配布済みであり、それぞれの端末ID1201、プログラムID1202、プログラム固有情報ID1203の組は、(端末ID, プログラムID, プログラム固有情報ID) = (0001, 0001, 0001)、(0002, 0001, 0002)、(0010, 0001, 0003)、(001
10 5, 0001, 0004)、(0020, 0002, 1001)となる。

また、プログラム／固有情報対応表保持部1150は、プログラム／固有情報対応表1210に、サーバ装置1120が管理しているプログラムのプログラムID1211と、各プログラムが使用するプログラム固有情報を識別するプログラム固有情報ID1212との対応関係を格
15 納する。

図12の例では、サーバ装置1120はプログラムIDが0001のプログラムを管理しており、そのプログラムが使用するプログラム固有情報としてプログラム固有情報IDが0001から1000までのプログラム固有情報を管理している。同様にプログラムIDが0002のプログラムと、そのプログラムが使用するプログラム固有情報IDが10
20 01から2000までのプログラム固有情報を管理している。また、プログラム／固有情報対応表1210には、情報処理端末1100に配布済みのプログラム固有情報の再配布を防止するために、次のプログラム固有情報配布の開始時に、配布すべきプログラム固有情報である配布
25 開始ID1213を格納する。

図12の例では、プログラムIDが0001のプログラムに対し新た

にプログラム固有情報を割り当てる場合、サーバ装置 1120 はプログラム固有情報 ID 0123 のプログラム固有情報を割り当てることを示している。同様にプログラム ID が 0002 のプログラムに対し新たにプログラム固有情報を割り当てる場合、サーバ装置 1120 はプログラム固有情報 ID 1423 のプログラム固有情報を割り当てることを示している。

また、サーバ装置 1120 は、このプログラム／固有情報対応表 1210 を用いて、情報処理端末 1100 からのプログラム ID を指定したプログラム配布要求に対し、そのプログラム ID に対応したプログラム固有情報を配布することとなる。

本発明の実施の形態 2 におけるプログラム配布手順について、図 13 を用いて説明する。図 13 は、サーバ装置 1120 におけるプログラムの配布手順を示すフローチャートである。

第 1 に、サーバ装置 1120 は情報処理端末 1100 からプログラム配布要求を受信する (S1301)。このプログラム配布要求は、プログラム ID を指定するものである。

次に、サーバ装置 1120 は、受信したプログラム配布要求から情報処理端末 1100 の端末 ID 及びプログラム ID を取得する (S1302)。そして、固有情報配布履歴 1200 に対して取得した端末 ID、プログラム ID を検索し (S1303)、固有情報配布履歴 1200 に同じ端末 ID かつ同じプログラム ID の履歴が格納されているか否か確認する (S1304)。

固有情報配布履歴 1200 に同じ端末 ID かつ同じプログラム ID の履歴が格納されていた場合には (S1304 で Y)、サーバ装置 1120 は、情報処理端末 1100 に既に指定プログラムに対するプログラム固有情報 1135 を配布済みであるため、プログラム 1133 のみを送

信し処理を終了する（S 1 3 0 9）。

固有情報配布履歴 1 2 0 0 に同じ端末 ID かつ同じプログラム ID の履歴が格納されていない場合には（S 1 3 0 4 で N）、サーバ装置 1 1 2 0 は、プログラム／固有情報対応表 1 2 1 0 に格納されている配布開始 ID の情報を元に情報処理端末 1 1 0 0 へ新たにプログラム固有情報 1 1 3 5 を割り当てる（S 1 3 0 5）。

次に、サーバ装置 1 1 2 0 は、新たに割り当てたプログラム固有情報 1 1 3 5 に関し、プログラム／固有情報対応表保持部 1 1 5 0 に格納されているプログラム／固有情報対応表 1 2 1 0 を参照して、配布開始 ID 1 2 1 3 の値を更新する（S 1 3 0 6）。また、新たに割り当てたプログラム固有情報 1 1 3 5 に関し、端末 ID とプログラム固有情報 ID の対応を固有情報配布履歴 1 2 0 0 に追加する（S 1 3 0 7）。そして、サーバ装置 1 1 2 0 は、プログラム固有情報 1 1 3 5 を情報処理端末 1 1 0 0 に送信し（S 1 3 0 8）、プログラム 1 1 3 3 を送信し処理を終了する（S 1 3 0 9）。

以上のように、本実施の形態 2 に係るサーバ装置 1 1 2 0 は、固有情報配布履歴保持部 1 1 4 0 とプログラム／固有情報対応表保持部 1 1 5 0 とを有し、固有情報配布履歴 1 2 0 0 とプログラム／固有情報対応表 1 2 1 0 を用いてプログラム固有情報の配布管理を行うことにより、1 つの情報処理端末 1 1 0 0 で動作する同一プログラムに対して複数のプログラム固有情報 1 1 3 5 を配布することを防ぐ。このため、新たなプログラム固有情報 1 1 3 5 を取得して排除の回避を図る情報処理端末 1 1 0 0 がプログラム固有情報 1 1 3 5 を新規取得することを防止することが可能となる。

また、本実施の形態 2 に係るサーバ装置 1 1 2 0 は、ダウンロード対象のプログラムと、当該プログラムが動作する情報処理端末 1 1 0 0 と

の対応をプログラム／固有情報対応表 1 2 1 0 に格納してプログラム固有情報 1 1 3 5 の配布をプログラム単位に管理することにより、プログラム毎にプログラム固有情報 1 1 3 5 の配布可否を判定することが可能となる。このため、サーバ装置 1 1 2 0 はプログラム／固有情報対応表 1 2 1 0 を参照して、プログラムを動作対象でない情報処理端末 1 1 0 0 に配布することを防止することが可能となる。

尚、本実施の形態 2 ではデータ格納部 1 1 0 6 とプログラム格納部 1 1 0 5 を別にしているが、同一の格納部としてもよい。また、本実施の形態 2 で示した固有情報配布履歴 1 2 0 0 の形式は一例であり、最終配布日付 1 2 0 4 を削除してもよいし、他の情報を付加してもよい。同様にプログラム／固有情報対応表 1 2 1 0 の形式も一例であり、配布開始 ID 1 2 1 3 を別の形式で管理してもよい。例えば、全プログラム固有情報 ID を格納したテーブルを持ち、各プログラム固有情報 ID に対して割り当て済みか否かを識別するフラグを設けることにより、プログラム固有情報 1 1 3 5 の配布状態を管理してもよい。

また、本実施の形態 2 では固有情報配布履歴 1 2 0 0 に記載されている端末 ID 1 2 0 1 に対してプログラム固有情報 1 1 3 5 の配布を拒否しているが、その情報処理端末 1 1 0 0 に対して既に配布済みのプログラム固有情報 1 1 3 5 を再度配布してもよい。また、本実施の形態 2 では情報処理端末 1 1 0 0 からの要求はプログラムの配布を伴うプログラム配布要求、又はプログラムの配布が伴わないプログラム固有情報配布要求とできる。

(実施の形態 3)

図 1 4 は、本実施の形態 3 に係る情報処理端末 1 4 0 0 とサーバ装置 1 4 2 0 の構成図を示す。同図において、前述した実施の形態 1 及び実施の形態 2 と異なる点は、サーバ装置 1 4 2 0 が配布回数情報保持部 1

440を有する点である。

この配布回数情報保持部1440は、サーバ装置1420から同一の情報処理端末1400に対してプログラム固有情報1435を配布した回数を管理するための配布回数情報1500を保持するハードディスク
5 である。

図15は、本実施の形態3に係る配布回数情報1500の情報格納例を示す図である。

配布回数情報1500には、プログラム固有情報1435を配布した情報処理端末1400を識別するIDである端末ID1501、配布した回数を示す回数カウンタ1502が格納される。同図の例では、端末
10 IDが0001、0002の情報処理端末1400に対してプログラム固有情報1435を1回配布しており、端末IDが0003の情報処理端末1400に対してプログラム固有情報1435を配布していないことが示されている。

15 図16は、サーバ装置1420におけるプログラムの配布手順を示すフローチャートである。

まず、サーバ装置1420は情報処理端末1400からプログラム配布要求を受信する(S1601)。次に、サーバ装置1420は、S1601で受信したプログラム配布要求に含まれる情報処理端末1400
20 の端末IDを取得する(S1602)。

そして、サーバ装置1420は配布回数情報保持部1440に保持される配布回数情報1500を用いてS1602で取得した端末IDを検索し、回数カウンタの値を取得する(S1603)。また、取得した回数カウンタの値が規定値以上か否かを判定する(S1604)。

25 そして、取得した回数カウンタの値が規定値以上であった場合(S1604でY)、サーバ装置1420は、情報処理端末1400に対して

は既にプログラム固有情報 1 4 3 5 を規定回数以上配布しているため、
プログラム 1 4 3 3 のみを送信し処理を終了する (S 1 6 0 8)。

一方、取得した回数カウンタの値が規定値未満であった場合 (S 1 6
0 4 で N)、サーバ装置 1 4 2 0 は情報処理端末 1 4 0 0 へは新たにプ
5 プログラム固有情報 1 4 3 5 を割り当てる (S 1 6 0 5)。また、サーバ
装置 1 4 2 0 は配布回数情報保持部 1 4 4 0 内に格納されている配布回
数情報 1 5 0 0 の回数カウンタの値を加算する (S 1 6 0 6)。そして、
サーバ装置 1 4 2 0 は、プログラム固有情報 1 4 3 5 を情報処理端末 1
4 0 0 に送信し (S 1 6 0 7)、プログラム 1 4 3 3 を送信し処理を終
10 了する (S 1 6 0 8)。

このように、本実施の形態 3 に係るサーバ装置 1 4 2 0 は、配布回数
情報保持部 1 4 4 0 を有し、配布回数情報 1 5 0 0 を用いてプログラム
固有情報 1 4 3 5 の配布管理を行うことにより、1 つの情報処理端末 1
4 0 0 へ規定値以上のプログラム固有情報 1 4 3 5 を配布することを防
15 ぐことができる。特に、規定値を 1 に設定した場合、本発明の実施の形
態 1 及び実施の形態 2 と同様に、サーバ装置 1 4 2 0 は、プログラム固
有情報 1 4 3 5 が含む情報を用いて不正端末と認識され、排除されてい
る情報処理端末 1 4 0 0 に対し、新たにプログラム固有情報 1 4 3 5 を
割り当てることにより、不正端末が排除を回避することを防ぐことが可
20 能となる。

また、プログラム固有情報 1 4 3 5 の配布回数を示す規定値を 2 以上
とすることにより、ハードディスクが故障したような不正の目的でなく
プログラムを再度購入するようなユーザに対してプログラム固有情報 1
4 3 5 の再配布や新たな配布を正規に行うことが可能となる。

25 尚、本実施の形態 3 ではデータ格納部 1 4 0 6 とプログラム格納部 1
4 0 5 を別にしているが、同一の格納部としてもよい。また、本実施の

形態 3 で示した配布回数情報 1 5 0 0 の形式は一例であり、他の情報を付加してもよい。また、本実施の形態 3 では情報処理端末 1 4 0 0 からの要求はプログラムの配布を伴うプログラム配布要求、又はプログラムの配布要求を伴わないプログラム固有情報配布要求とできる。

5 (実施の形態 4)

図 1 7 は、本実施の形態 4 に係る情報処理端末 1 7 0 0 とサーバ装置 1 7 2 0 の構成図を示す。同図において、前述の実施の形態 3 と異なる点は、サーバ装置 1 7 2 0 がプログラム／固有情報対応表保持部 1 7 5 0 を保持する点である。このプログラム／固有情報対応表保持部 1 7 5 0 は、図 1 1 において説明したプログラム／固有情報対応表保持部 1 1 5 0 と同様の記憶部である。

図 1 8 (a) 及び (b) は、本実施の形態 4 に係る配布回数情報 1 8 0 0 とプログラム／固有情報対応表 1 8 1 0 に格納されるデータの一例を示す図である。

15 配布回数情報 1 8 0 0 は、配布したプログラムのプログラム ID 1 8 0 1、プログラム固有情報 1 7 3 5 を配布した情報処理端末 1 7 0 0 の端末 ID 1 8 0 2、プログラム固有情報を配布した回数を示す回数カウンタ 1 8 0 3 を格納する。前記実施の形態 3 における配布回数情報 1 5 0 0 と異なる点は、プログラム固有情報を使用するプログラムを識別するプログラム ID 1 8 0 1 が付加されている点である。

20 配布回数情報 1 8 0 0 は、プログラム ID が 0 0 0 1 のプログラムが使用するプログラム固有情報 1 7 3 5 を、端末 ID が 0 0 0 1、0 0 0 2 の情報処理端末 1 7 0 0 に対して 1 回配布し、端末 ID が 0 0 0 3 の情報処理端末 1 7 0 0 に対してプログラム固有情報 1 7 3 5 を配布していないことを示す。また同様に、プログラム ID が 0 0 0 2 のプログラムが使用するプログラム固有情報 1 7 3 5 を、端末 ID が 0 0 0 1 の情

報処理端末 1700 に対して 1 回配布しており、端末 ID が 0002、
0003 の情報処理端末 1700 に対してプログラム固有情報 1735
を配布していないことを示している。

5 尚、プログラム／固有情報対応表 1810 は、前述した図 12 におけ
るプログラム／固有情報対応表 1210 と同様であり、詳細な説明は省
略する。

図 19 は、サーバ装置 1720 におけるプログラムの配布手順を示す
フローチャートである。

まず、サーバ装置 1720 は情報処理端末 1700 からプログラム配
10 布要求を受信する (S1901)。このプログラム配布要求には、情報
処理端末 1700 より取得の要求されるプログラムのプログラム ID を
含む。次に、サーバ装置 1720 は、S1901 で受信したプログラム
配布要求に含まれる情報処理端末 1700 の端末 ID、プログラム ID
を取得する (S1902)。

15 そして、サーバ装置 1720 は、配布回数情報 1800 に対して S1
902 で取得した端末 ID、プログラム ID を検索し、回数カウンタの
値を取得する (S1903)。次に、取得した回数カウンタの値が規定
値以上か否かを判定する (S1904)。

また、取得した回数カウンタの値が規定値以上であった場合 (S19
20 04 で Y)、サーバ装置 1720 は、情報処理端末 1700 へは既にプ
ログラム固有情報 1735 を規定回数以上配布しているため、プログラ
ム 1733 のみを送信し処理を終了する (S1909)。

次に、取得した回数カウンタの値が規定値未満であった場合 (S19
04 で N)、サーバ装置 1720 は、プログラム／固有情報対応表 18
25 10 に格納されている配布開始 ID の情報を元に情報処理端末 1700
へ新たにプログラム固有情報 1735 を割り当てる (S1905)。

そして、サーバ装置 1720 は、S1905 で新たに割り当てたプログラム固有情報 1735 に関し、プログラム／固有情報対応表 1810 に格納されている配布開始 ID の値を更新する (S1906)。また、配布回数情報 1800 内に格納されている回数カウンタの値を加算し
5 (S1907)、プログラム固有情報 1735 を情報処理端末 1700 に送信し (S1908)、プログラム 1733 を送信し処理を終了する (S1909)。

以上のように、本実施の形態 4 に係るサーバ装置 1720 は、配布回数情報保持部 1740 とプログラム／固有情報対応表保持部 1750 と
10 を有し、各保持部に保持される配布回数情報 1800 及びプログラム／固有情報対応表 1810 を用いてプログラム固有情報 1735 を配布管理することにより、1 つの情報処理端末 1700 で動作する同一プログラムに対して規定値以上のプログラム固有情報 1735 を配布することを防いで、プログラム固有情報 1735 の不正使用を図る情報処理端末
15 1700 を排除することが可能となる。

また、本実施の形態 4 では、サーバ装置 1720 は、プログラム固有情報の配布をプログラム単位に管理することにより、プログラム毎にプログラム固有情報 1735 の配布可否を判定することが可能となる。

尚、本実施の形態 4 ではデータ格納部 1706 とプログラム格納部 1
20 705 を別にしているが、同一の格納部としてもよい。また、本実施の形態 4 で示した配布回数情報 1800 の形式は一例であり、他の情報を付加してもよい。同様にプログラム／固有情報対応表 1810 の形式も一例であり、別の形式で管理してもよい。また、本実施の形態 4 では情報処理端末 1700 からの要求はプログラムの配布を伴うプログラム配布要求、又はプログラムの配布を伴わないプログラム固有情報配布要求
25 とできる。

以上のように、本発明に係るサーバ装置は、固有情報配布履歴保持部を有することにより、情報処理端末が以前に配布したプログラムに対応するプログラム固有情報の新規取得を防止することが可能となり、新たなプログラム固有情報を取得して排除の回避を図る情報処理端末の不正行為を確実に防止することが可能となる。

また、本発明に係る情報処理端末は、サーバ装置から取得したプログラムを端末固有鍵で暗号化することにより、サーバ装置におけるプログラム暗号化処理の負担を軽減することが可能となる。さらに、本発明に係るサーバ装置は、プログラム全体をプログラム及びプログラム固有情報に分離して個別に作成しているため、サーバ装置は、各情報処理端末で異なる情報となる容量の比較的小さなプログラム固有情報を複数管理して、全情報処理端末で共通な情報となる容量の大きなプログラムは1つのみ管理して、サーバ装置で管理する配布情報の容量を低減することが可能となり、情報管理の負担を軽減することが可能となる。

そして、本発明に係るサーバ装置から情報処理端末に配布されるプログラムの全体には、情報処理端末で動作するプログラム本体、プログラムヘッダ、プログラム固有情報、及び固有情報ヘッダが含まれるため、プログラムを構成する各情報にCA署名やハッシュ値を用いることにより、サーバ装置から情報処理端末に配布される情報の正当性を確認することが可能となる。

産業上の利用の可能性

本発明に係るサーバ装置及びプログラム管理システムは、通信機能を備えるパーソナルコンピュータ、携帯電話等の情報処理端末にネットワークを介してプログラムを配布するサーバ装置、及び当該サーバ装置と情報処理端末との間のプログラム管理システムとして有用である。

請 求 の 範 囲

1. 外部から書き換えが行えない端末IDを保持する情報処理端末とネットワークを介して接続され前記情報処理端末で動作するプログラムを保持するサーバ装置であって、

以前に配布したプログラムと端末IDとの関連を示すテーブルを保持するテーブル保持手段と、

- 前記テーブルを参照して、前記情報処理端末から送信され前記端末IDを伴うプログラム取得要求に対するプログラムの配布をするか否かを判定する判定手段とを備える

ことを特徴とするサーバ装置。

2. 前記プログラムには、前記情報処理端末で動作するプログラム本体、及び当該プログラム本体に使用される固有の情報であるプログラム固有情報が含まれ、

- 15 前記判定手段は、

前記プログラム取得要求に付与されている前記端末IDが前記テーブルに記録されている場合には、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、

- 前記端末IDが前記テーブルに記載されていない場合には、前記端末IDと前記プログラム固有情報とを対応させて前記テーブルに追加すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する

ことを特徴とする請求項1記載のサーバ装置。

3. 前記判定手段は、
- 25 前記情報処理端末からの前記プログラム取得要求に対して、前記プログラム本体の配布は前記プログラム取得要求毎に行うと判定する一方、

前記プログラム固有情報の配布は 1 回のみ行うと判定する

ことを特徴とする請求項 2 記載のサーバ装置。

4. 前記テーブル保持手段は、

前記端末 ID と前記プログラム固有情報の配布回数とを示すテーブル

5 を保持し、

前記判定手段は、

前記テーブルを参照して、前記情報処理端末より配布された前記プログラム取得要求に付与されている前記端末 ID に対応する配布回数が規定値に達している場合においては、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、

10

前記テーブルを参照して、前記情報処理端末より配布された前記プログラム取得要求に付与されている前記端末 ID に対応する配布回数が規定値に達していない場合においては、前記端末 ID に対応させて前記テーブルに記載されている配布回数を更新すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する

15

ことを特徴とする請求項 1 記載のサーバ装置。

5. 前記テーブル保持手段は、

20 前記情報処理端末からのプログラム取得要求に付与されている前記端末 ID と、前記端末 ID の情報処理端末に配布した前記プログラム本体を一意に特定するプログラム本体 ID と、前記端末 ID の情報処理端末にプログラム固有情報を配布した回数とを示す配布回数との関連を示すテーブルを保持し、

25 前記判定手段は、

前記テーブルを参照して、前記情報処理端末より配布された前記プロ

グラム取得要求に付与されている前記端末IDと前記プログラムIDとの両方に対応する配布回数が規定値に達している場合においては、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、

- 5 前記テーブルを参照して、前記情報処理端末より配布された前記プログラム取得要求に付与されている前記端末ID及び前記プログラムIDに対応する配布回数が規定値に達していない場合においては、前記端末IDと前記プログラムIDとに対応させて前記テーブルに記載されている配布回数を更新すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する

ことを特徴とする請求項4記載のサーバ装置。

6. 前記規定値は、前記サーバ装置から前記情報処理端末に配布するプログラム固有情報の配布回数を示す値である

ことを特徴とする請求項4又は請求項5記載のサーバ装置。

- 15 7. 前記テーブル保持手段は、

前記情報処理端末からのプログラム取得要求に付与されている前記端末IDと、前記端末IDの情報処理端末に配布した前記プログラム本体を一意に特定するプログラム本体IDと、前記端末IDの情報処理端末に配布したプログラム固有情報を一意に特定するプログラム固有情報IDとの関連を示すテーブルを保持し、

- 20

前記判定手段は、

- 前記テーブルを参照して、前記情報処理端末より送信された前記プログラム取得要求に付与されている前記端末IDと前記プログラムIDとの両方に対応するプログラム固有情報IDが記載されている場合においては、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、
- 25

前記テーブルを参照して、前記プログラム取得要求に付与されている前記端末IDと前記プログラムIDとの両方に対応するプログラム固有情報IDが記載されていない場合においては、前記端末IDと前記プログラム固有情報IDと前記プログラムIDとを対応させて前記テーブルに追加すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する

ことを特徴とする請求項1記載のサーバ装置。

8. 前記サーバ装置は、

前記情報処理端末毎に異なる情報となる前記プログラム固有情報を複数保持し、

前記情報処理端末で共通な前記プログラム本体を1つ保持する

ことを特徴とする請求項2記載のサーバ装置。

9. 前記テーブル保持手段は、

前記プログラム本体を一意に特定するプログラム本体IDと、前記プログラム本体が動作する前記情報処理端末の端末IDとの関連を示すテーブルを保持し、

前記判定手段は、

前記テーブルを参照して、前記情報処理端末より配布された前記プログラム取得要求に付与されている前記端末IDと前記プログラムIDとが対応して記載されている場合においては、前記プログラムの配布可能と判定し、

前記テーブルを参照して、前記プログラム取得要求に付与されている前記端末IDと前記プログラムIDとが対応して記載されていない場合においては、前記プログラム本体の配布不可と判定する

ことを特徴とする請求項2記載のサーバ装置。

10. 外部から書き換えが行えない端末IDを保持する情報処理端末

と、当該情報処理端末とネットワークを介して接続され前記情報処理端末で動作するプログラムを保持するサーバ装置とから構成されるプログラム管理システムであって、

前記情報処理端末は、

- 5 前記プログラムの取得を要求する場合には、前記端末IDを付与したプログラム取得要求を前記サーバ装置に送信し、

前記サーバ装置は、

前記プログラム取得要求を受信して、以前に配布したプログラムと端末IDとの関連を示すテーブルを保持するテーブル保持手段と、

- 10 前記テーブルを参照して、前記情報処理端末から送信されて前記端末IDが付与されているプログラム取得要求に対するプログラムの配布をするか否かを判定する判定手段とを備える

ことを特徴とするプログラム管理システム。

11. 前記情報処理端末は、外部から書き換えが行えないメモリ部に

- 15 前記情報処理端末毎に異なる固有鍵を格納し、

前記サーバ装置から取得した前記プログラムを、前記固有鍵を用いて暗号化して前記情報処理端末内のメモリ部に格納する格納手段を備える

ことを特徴とする請求項10記載のプログラム管理システム。

12. 前記プログラムには、前記情報処理端末で動作するプログラム

- 20 本体、当該プログラム本体に関する情報を格納するプログラムヘッダ、前記プログラム本体に使用される固有の情報であるプログラム固有情報、及び当該プログラム固有情報に関する情報を格納した固有情報ヘッダが含まれ、

前記情報処理端末は、

- 25 前記サーバ装置に取得を要求するプログラムに含まれる前記プログラムヘッダ及び前記固有情報ヘッダの取得を要求するヘッダ取得要求を行

い、

前記サーバ装置は、

前記判定手段において前記プログラム本体の配布可能と判定される場合においては、前記プログラムヘッダ及び前記固有情報ヘッダを前記情

5 報処理端末に配布し、

前記情報処理端末は、

前記プログラムヘッダ及び前記固有情報ヘッダに基づいて検証を行う
検証手段を備え、当該検証手段での検証を行った後に前記プログラム取
得要求を前記サーバ装置に送信する

10 ことを特徴とする請求項 10 記載のプログラム管理システム。

13. 前記プログラムヘッダには、前記プログラムを一意に特定する
ことが可能な認証子が含まれ、

前記情報処理端末は、前記固有鍵で暗号化され前記情報処理端末内の
メモリ部に格納されているプログラムを前記固有鍵で復号し、前記認証
15 子を用いて前記固有鍵での暗号化が正しく行われたことを検証する検証
手段を備える

ことを特徴とする請求項 12 記載のプログラム管理システム。

14. 前記プログラム、前記プログラムヘッダ、前記プログラム固有
情報、及び前記固有情報ヘッダには電子的な署名が付加されている

20 ことを特徴とする請求項 12 記載のプログラム管理システム。

15. 前記プログラムヘッダには、前記プログラムを一意に特定する
ことが可能な認証子が含まれ、前記固有情報ヘッダには、前記プログラ
ム固有情報を一意に特定することが可能な認証子が含まれる

ことを特徴とする請求項 12 記載のプログラム管理システム。

25 16. 外部から書き換えが行えない端末 ID を保持する情報処理端末
と、当該情報処理端末とネットワークを介して接続され前記情報処理端

末で動作するプログラムを保持するサーバ装置とから構成されるプログラム配布方法であって、

前記情報処理端末は、

- 前記プログラムの取得を要求する場合には、前記端末IDを付与した
- 5 プログラム取得要求を前記サーバ装置に送信するステップを有し、

前記サーバ装置は、

前記プログラム取得要求を受信して、以前に配布したプログラムと端末IDとの関連を示すテーブルを保持するテーブル保持ステップと、

- 前記テーブルを参照して、前記情報処理端末から送信されて前記端末
- 10 IDが付与されているプログラム取得要求に対するプログラムの配布をするか否かを判定する判定ステップとを有する

ことを特徴とするプログラム配布方法。

17. 外部から書き換えが行えない端末IDを保持する情報処理端末とネットワークを介して接続され前記情報処理端末で動作する配布プログラムを保持するサーバ装置で用いられるプログラムであって、
- 15

以前に配布した配布プログラムと端末IDとの関連を示すテーブルを保持するテーブル保持ステップと、

- 前記テーブルを参照して、前記情報処理端末から送信され前記端末IDを伴うプログラム取得要求に対する配布プログラムの配布をするか否
- 20 かを判定する判定ステップとをコンピュータに実行させる

ことを特徴とするプログラム。

補正書の請求の範囲

[2003年10月7日(07.10.03)国際事務局受理:出願当初の請求の範囲1,10,16及び17は取り下げられた;新しい請求の範囲18及び19が加えられた;他の請求の範囲は変更なし。(7頁)]

1. (削除)

2. (補正後) 外部から書き換えが行えない端末IDを保持する情報処理端末とネットワークを介して接続され、

以前に配布したプログラムと端末IDとの関連を示すテーブルを参照して、前記情報処理端末から送信された前記端末IDを伴うプログラム取得要求に対するプログラムの配布をするか否かを判定するサーバ装置であって、

- 10 前記プログラムには、前記情報処理端末で動作するプログラム本体、及び当該プログラム本体に使用される固有の情報であるプログラム固有情報が含まれ、

- 前記プログラム取得要求に付与されている前記端末IDが前記テーブルに記録されている場合には、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、

- 15 前記端末IDが前記テーブルに記載されていない場合には、前記端末IDと前記プログラム固有情報とを対応させて前記テーブルに追加すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する判定手段を備える

- 20 ことを特徴とするサーバ装置。

3. 前記判定手段は、

前記情報処理端末からの前記プログラム取得要求に対して、前記プログラム本体の配布は前記プログラム取得要求毎に行うと判定する一方、前記プログラム固有情報の配布は1回のみ行うと判定する

- 25 ことを特徴とする請求項2記載のサーバ装置。

4. (補正後) 前記テーブル保持手段は、

前記端末IDと前記プログラム固有情報の配布回数とを示すテーブルを保持し、

前記判定手段は、

- 前記テーブルを参照して、前記情報処理端末より配布された前記プログラム取得要求に付与されている前記端末IDに対応する配布回数が規定値に達している場合においては、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、

- 前記テーブルを参照して、前記情報処理端末より配布された前記プログラム取得要求に付与されている前記端末IDに対応する配布回数が規定値に達していない場合においては、前記端末IDに対応させて前記テーブルに記載されている配布回数を更新すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する

- 15 ことを特徴とする請求項2記載のサーバ装置。

5. 前記テーブル保持手段は、

- 前記情報処理端末からのプログラム取得要求に付与されている前記端末IDと、前記端末IDの情報処理端末に配布した前記プログラム本体を一意に特定するプログラム本体IDと、前記端末IDの情報処理端末にプログラム固有情報を配布した回数とを示す配布回数との関連を示すテーブルを保持し、

前記判定手段は、

- 前記テーブルを参照して、前記情報処理端末より配布された前記プログラム取得要求に付与されている前記端末IDと前記プログラムIDとの両方に対応する配布回数が規定値に達している場合においては、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を

前記情報処理端末に行うと判定し、

前記テーブルを参照して、前記情報処理端末より配布された前記プログラム取得要求に付与されている前記端末ID及び前記プログラムID
5 IDと前記プログラムIDとに対応させて前記テーブルに記載されている配布回数を更新すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する

ことを特徴とする請求項4記載のサーバ装置。

6. 前記規定値は、前記サーバ装置から前記情報処理端末に配布する
10 プログラム固有情報の配布回数を示す値である

ことを特徴とする請求項4又は請求項5記載のサーバ装置。

7. (補正後) 前記テーブル保持手段は、

前記情報処理端末からのプログラム取得要求に付与されている前記端末IDと、前記端末IDの情報処理端末に配布した前記プログラム本体
15 を一意に特定するプログラム本体IDと、前記端末IDの情報処理端末に配布したプログラム固有情報を一意に特定するプログラム固有情報IDとの関連を示すテーブルを保持し、

前記判定手段は、

前記テーブルを参照して、前記情報処理端末より送信された前記プログラム取得要求に付与されている前記端末IDと前記プログラムIDとの
20 の両方に対応するプログラム固有情報IDが記載されている場合においては、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、

前記テーブルを参照して、前記プログラム取得要求に付与されている
25 前記端末IDと前記プログラムIDとの両方に対応するプログラム固有情報IDが記載されていない場合においては、前記端末IDと前記プロ

グラム固有情報IDと前記プログラムIDとを対応させて前記テーブルに追加すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する

ことを特徴とする請求項2記載のサーバ装置。

5 8. 前記サーバ装置は、

前記情報処理端末毎に異なる情報となる前記プログラム固有情報を複数保持し、

前記情報処理端末で共通な前記プログラム本体を1つ保持する

ことを特徴とする請求項2記載のサーバ装置。

10 9. 前記テーブル保持手段は、

前記プログラム本体を一意に特定するプログラム本体IDと、前記プログラム本体が動作する前記情報処理端末の端末IDとの関連を示すテーブルを保持し、

前記判定手段は、

15 前記テーブルを参照して、前記情報処理端末より配布された前記プログラム取得要求に付与されている前記端末IDと前記プログラムIDとが対応して記載されている場合においては、前記プログラムの配布可能と判定し、

前記テーブルを参照して、前記プログラム取得要求に付与されている
20 前記端末IDと前記プログラムIDとが対応して記載されていない場合においては、前記プログラム本体の配布不可と判定する

ことを特徴とする請求項2記載のサーバ装置。

10. (削除)

11. (補正後) 外部から書き換えが行えない端末IDを保持する情報
25 処理端末と、

以前に配布したプログラムと端末IDとの関連を示すテーブルを参照

して、前記情報処理端末から送信された前記端末IDを伴うプログラム取得要求に対するプログラムの配布をするか否かを判定するサーバ装置とがネットワークを介して接続して構成されるプログラム管理システムであって、

- 5 前記情報処理端末は、外部から書き換えが行えないメモリ部に前記情報処理端末毎に異なる固有鍵を格納し、

前記サーバ装置から取得した前記プログラムを、前記固有鍵を用いて暗号化して前記情報処理端末内のメモリ部に格納する格納手段を備えることを特徴とするプログラム管理システム。

- 10 12. (補正後) 前記プログラムには、前記情報処理端末で動作するプログラム本体、当該プログラム本体に関する情報を格納するプログラムヘッダ、前記プログラム本体に使用される固有の情報であるプログラム固有情報、及び当該プログラム固有情報に関する情報を格納した固有情報ヘッダが含まれ、

- 15 前記情報処理端末は、

前記サーバ装置に取得を要求するプログラムに含まれる前記プログラムヘッダ及び前記固有情報ヘッダの取得を要求するヘッダ取得要求を行い、

前記サーバ装置は、

- 20 前記判定手段において前記プログラム本体の配布可能と判定される場合においては、前記プログラムヘッダ及び前記固有情報ヘッダを前記情報処理端末に配布し、

前記情報処理端末は、

前記プログラムヘッダ及び前記固有情報ヘッダに基づいて検証を行う

- 25 検証手段を備え、当該検証手段での検証を行った後に前記プログラム取得要求を前記サーバ装置に送信する

ことを特徴とする請求項 1 1 記載のプログラム管理システム。

1 3. 前記プログラムヘッダには、前記プログラムを一意に特定することが可能な認証子が含まれ、

5 前記情報処理端末は、前記固有鍵で暗号化され前記情報処理端末内のメモリ部に格納されているプログラムを前記固有鍵で復号し、前記認証子を用いて前記固有鍵での暗号化が正しく行われたことを検証する検証手段を備える

ことを特徴とする請求項 1 2 記載のプログラム管理システム。

1 4. 前記プログラム、前記プログラムヘッダ、前記プログラム固有
10 情報、及び前記固有情報ヘッダには電子的な署名が付加されている

ことを特徴とする請求項 1 2 記載のプログラム管理システム。

1 5. 前記プログラムヘッダには、前記プログラムを一意に特定することが可能な認証子が含まれ、前記固有情報ヘッダには、前記プログラム固有情報を一意に特定することが可能な認証子が含まれる

15 ことを特徴とする請求項 1 2 記載のプログラム管理システム。

1 6. (削除)

1 7. (削除)

1 8. (追加) 外部から書き換えが行えない端末 ID を保持する情報処理端末とネットワークを介して接続され、

20 以前に配布したプログラムと端末 ID との関連を示すテーブルを参照して、前記情報処理端末から送信された前記端末 ID を伴うプログラム取得要求に対するプログラムの配布をするか否かを判定するサーバ装置で用いられるプログラム配布方法であって、

前記プログラムには、前記情報処理端末で動作するプログラム本体、
25 及び当該プログラム本体に使用される固有の情報であるプログラム固有情報が含まれ、

前記プログラム取得要求に付与されている前記端末IDが前記テーブルに記録されている場合には、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、

- 5 前記端末IDが前記テーブルに記載されていない場合には、前記端末IDと前記プログラム固有情報とを対応させて前記テーブルに追加すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する判定ステップを含む

ことを特徴とするプログラム配布方法。

19. (追加) 外部から書き換えが行えない端末IDを保持する情報処理10 端末とネットワークを介して接続され、

以前に配布したプログラムと端末IDとの関連を示すテーブルを参照して、前記情報処理端末から送信された前記端末IDを伴うプログラム取得要求に対するプログラムの配布をするか否かを判定するサーバ装置で用いられるプログラムであって、

- 15 前記プログラムには、前記情報処理端末で動作するプログラム本体、及び当該プログラム本体に使用される固有の情報であるプログラム固有情報が含まれ、

- 前記プログラム取得要求に付与されている前記端末IDが前記テーブルに記録されている場合には、前記プログラム固有情報の配布を禁止して前記プログラム本体のみの配布を前記情報処理端末に行うと判定し、20

前記端末IDが前記テーブルに記載されていない場合には、前記端末IDと前記プログラム固有情報とを対応させて前記テーブルに追加すると共に、前記プログラム本体と前記プログラム固有情報とを前記情報処理端末に配布すると判定する判定ステップを含む

- 25 ことを特徴とするプログラム。

条約第 19 条 (1) に基づく説明書

請求の範囲第 2 項は、サーバ装置が保持するプログラムには、プログラム本体、プログラム固有情報が含まれることを明確にし、また、サーバ装置の判定手段は端末 ID を用いてプログラム固有情報の配布を管理
5 することを明確にした。

請求の範囲第 4 項、7 項は、従属先である第 1 項を削除したため、第 2 項に従属させた。

10

請求の範囲第 11 項は、従属先である第 10 項を削除したために、プリアンブル部を補足すると共に、独立クレームとした。

請求の範囲第 12 項は、従属先である第 10 項を削除したために、請求の範囲第 11 項に従属させた。
15

請求の範囲第 1 項の削除に伴い、対応するプログラム配布方法及びプログラムである第 16 項及び第 17 項を削除した。また、新たに請求の範囲第 2 項に対応するプログラム配布方法及びプログラムに対応する請求の範囲第 18 項及び第 19 項を追加した。
20

出願人は、請求の範囲 1、10、16、17 を削除し、請求の範囲 2、4、7、11、12 を補正し、請求の範囲 3、5、6、8、9、13、14、15 は変更なく、新たに請求の範囲 18 及び 19 項を追加した。

25

図1

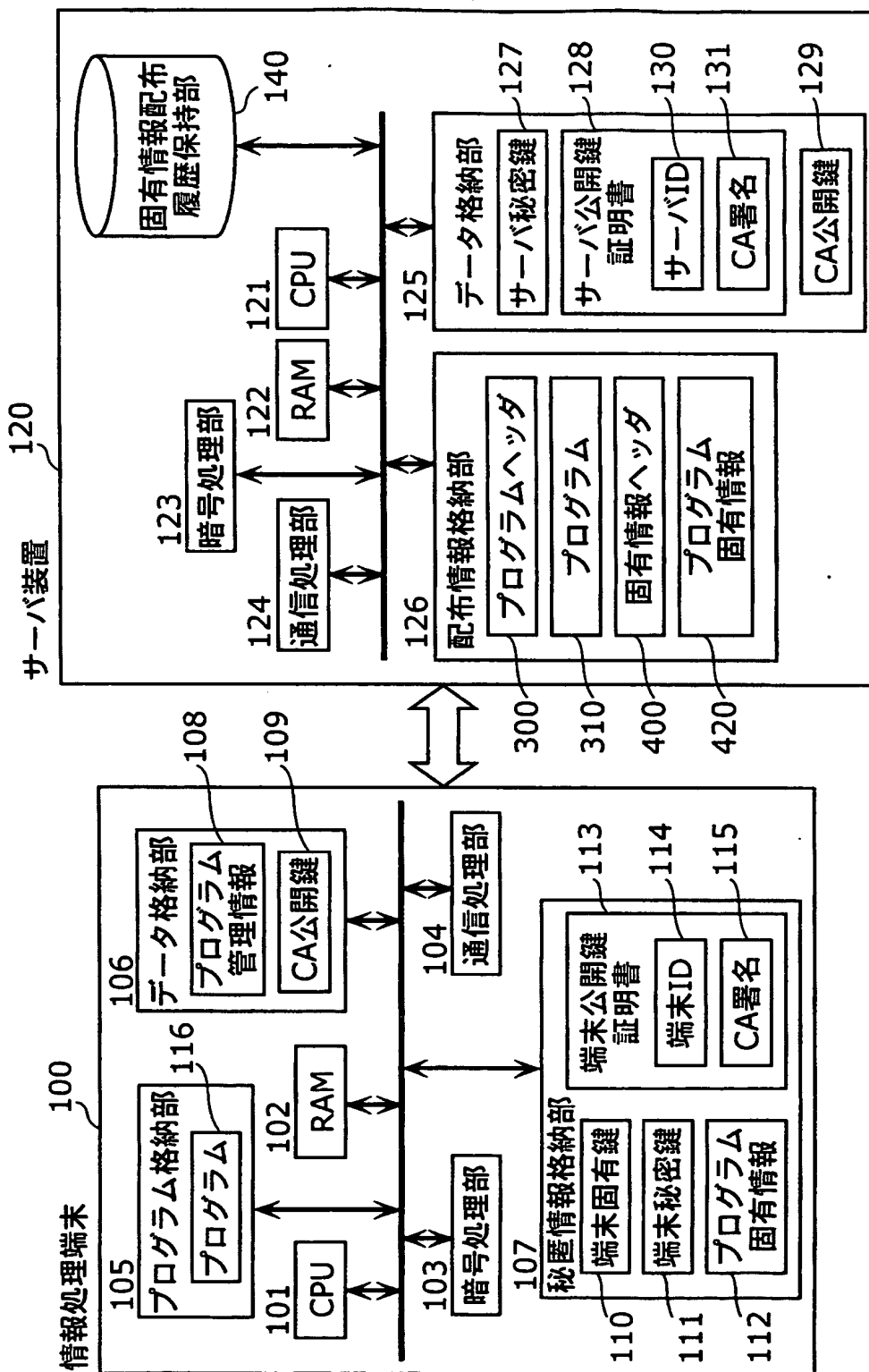


図2

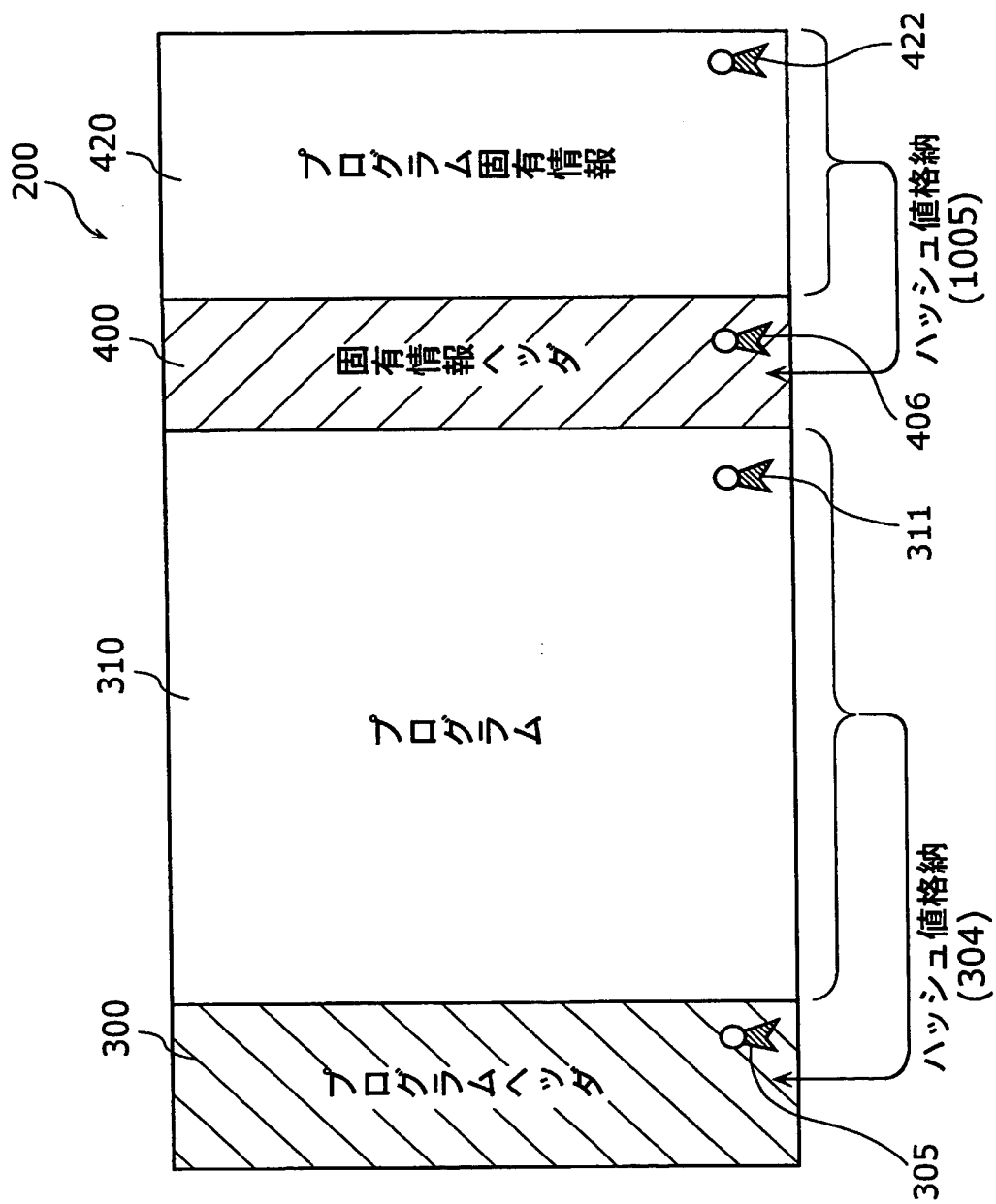


図3

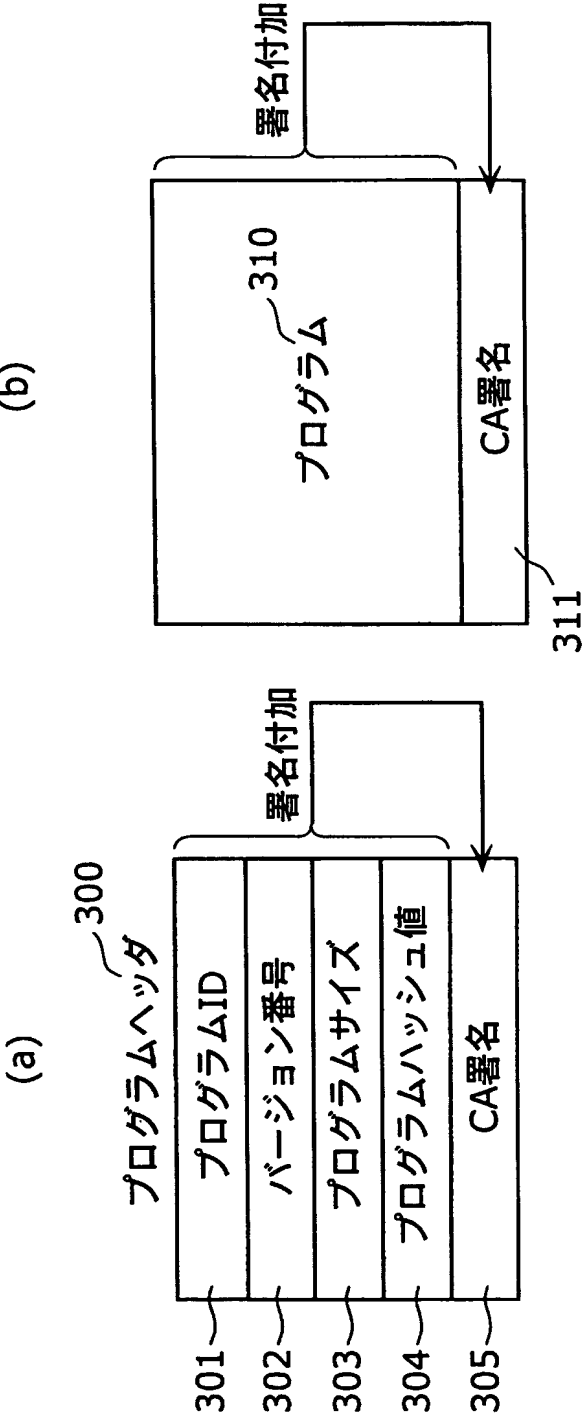


図4

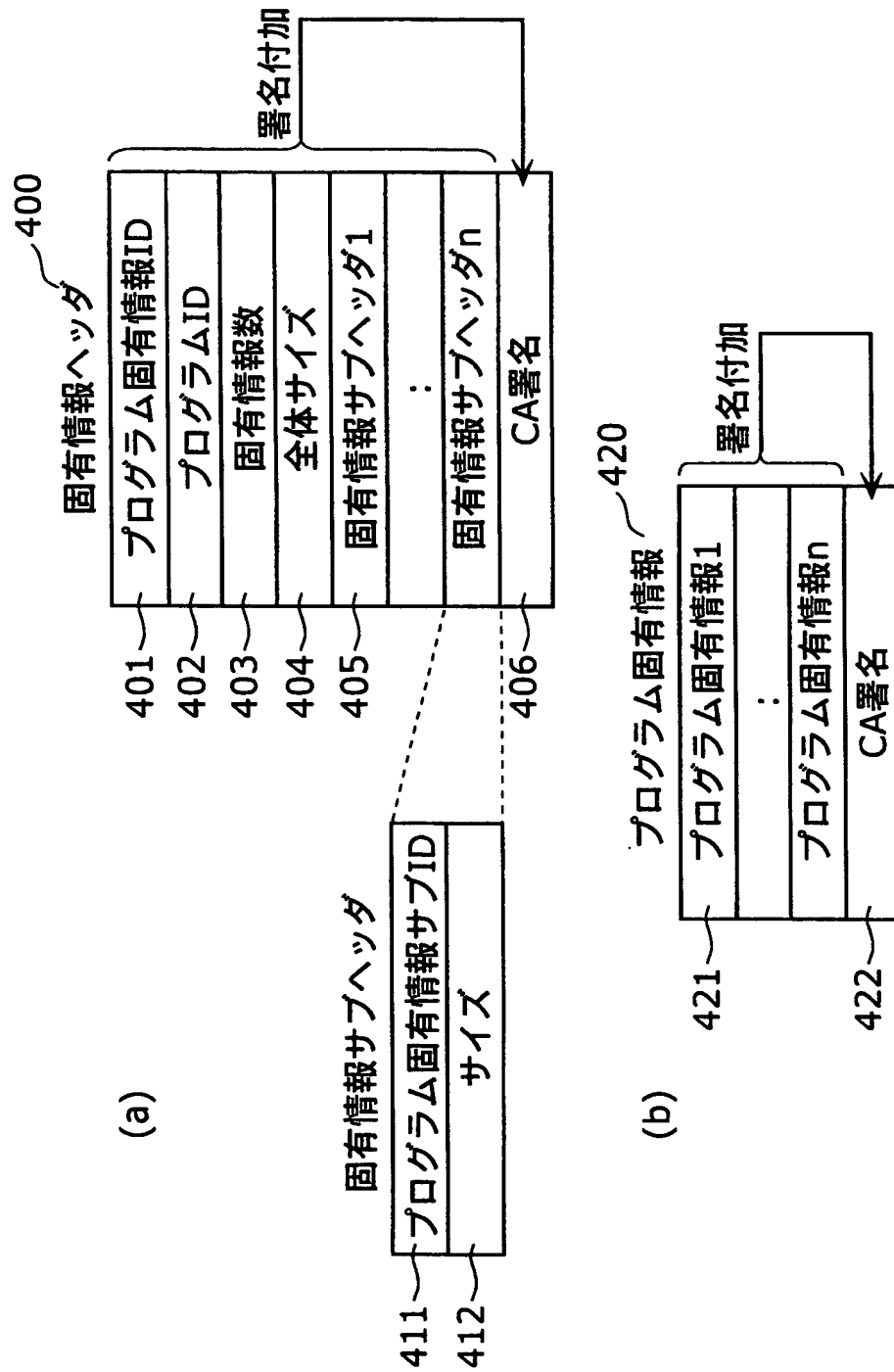


図5

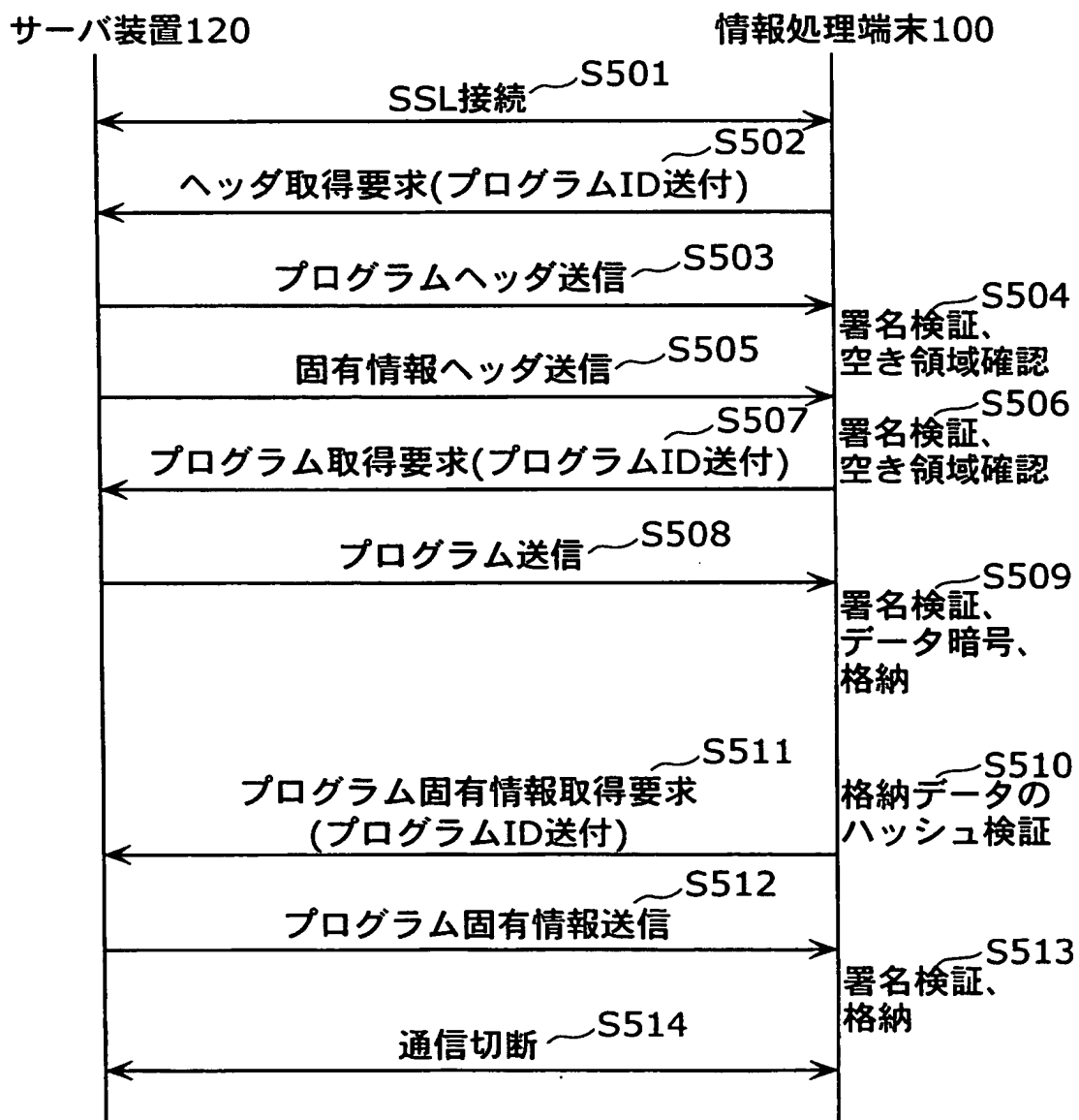


図6

固有情報配布履歴 600

601 端末ID	602 プログラム 固有情報ID	603 最終配布日付
0001	0001	2002.3.12
0002	0002	2002.3.12
0010	0003	2002.3.13
0015	0004	2002.3.14
0020	0005	2002.3.14

図7

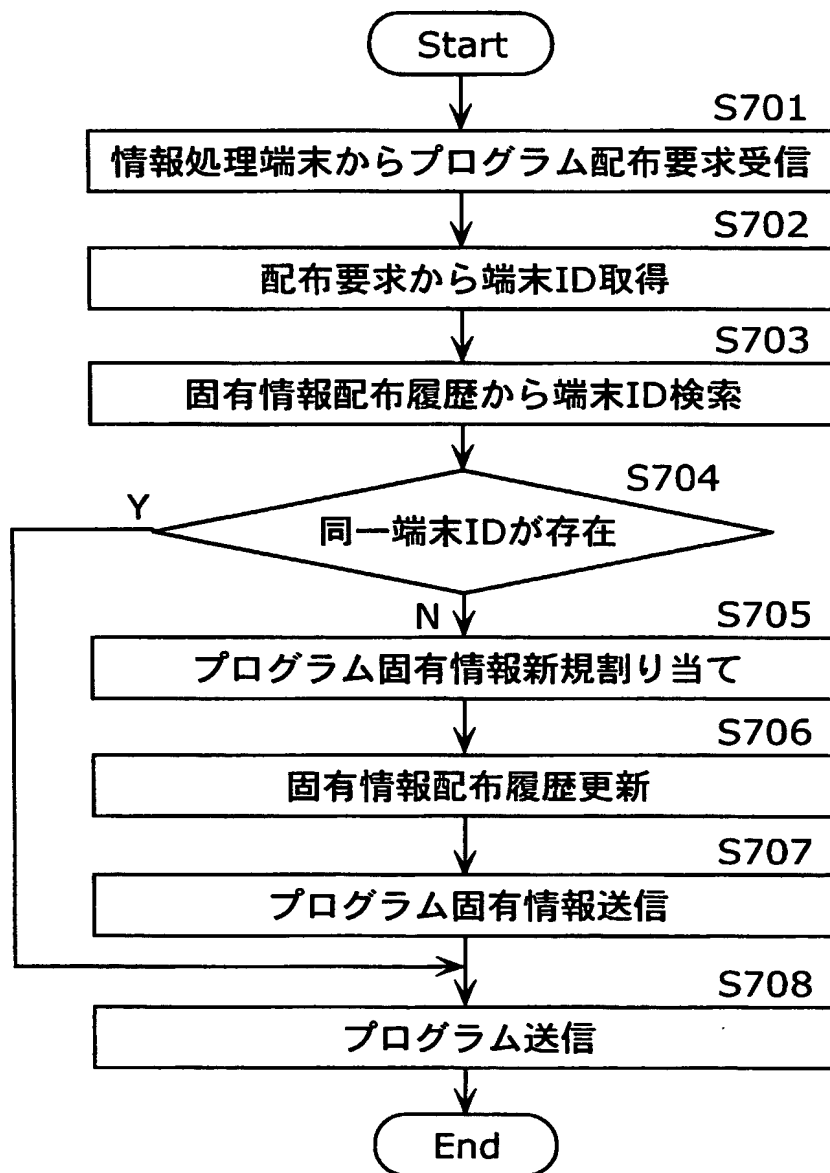


図8

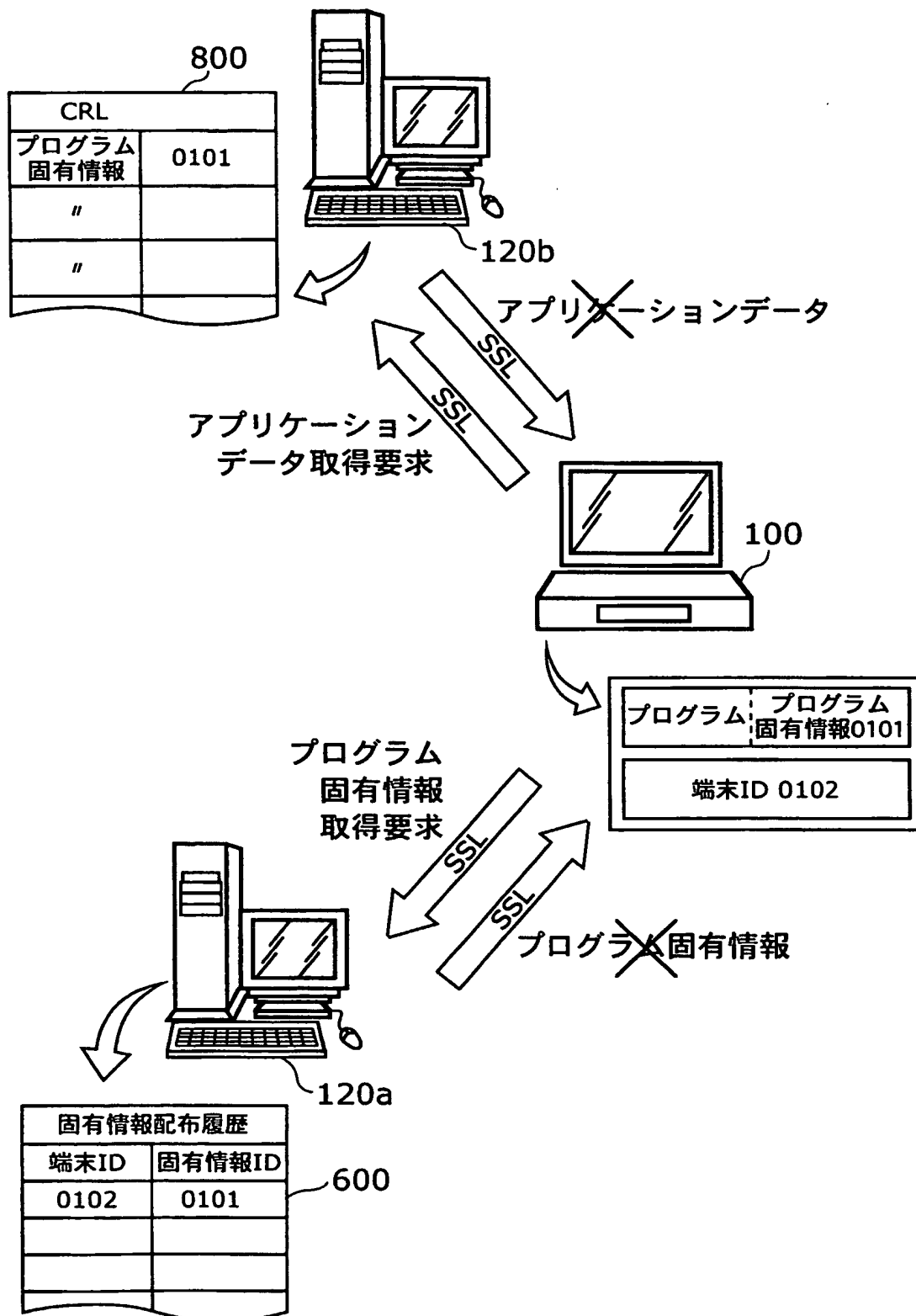


図9

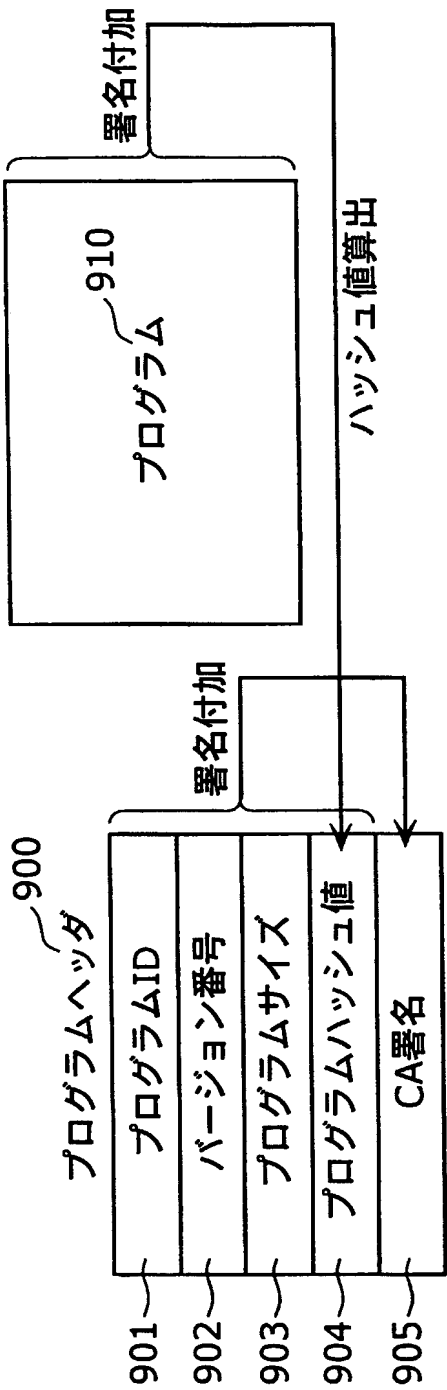


図10

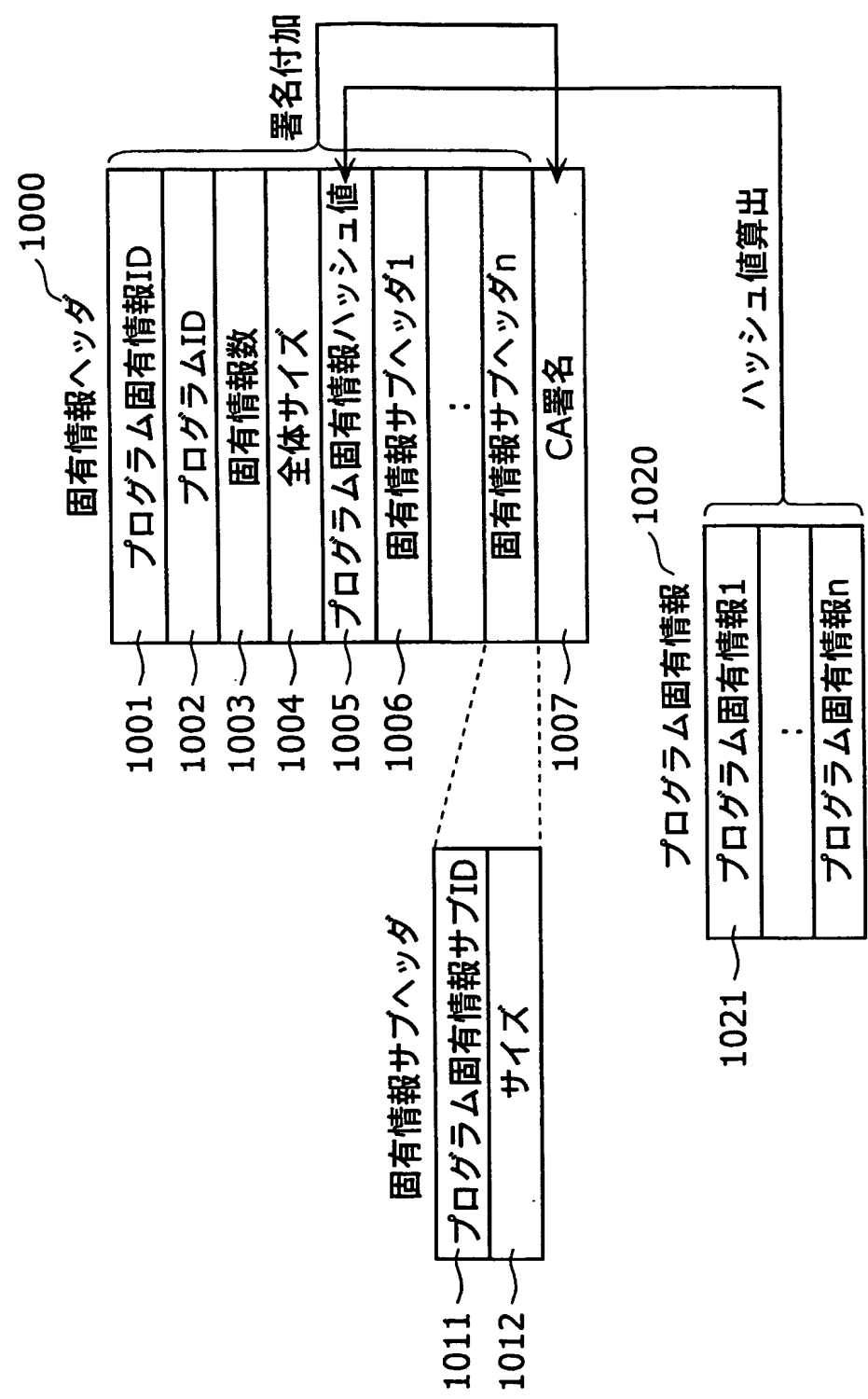


図 11

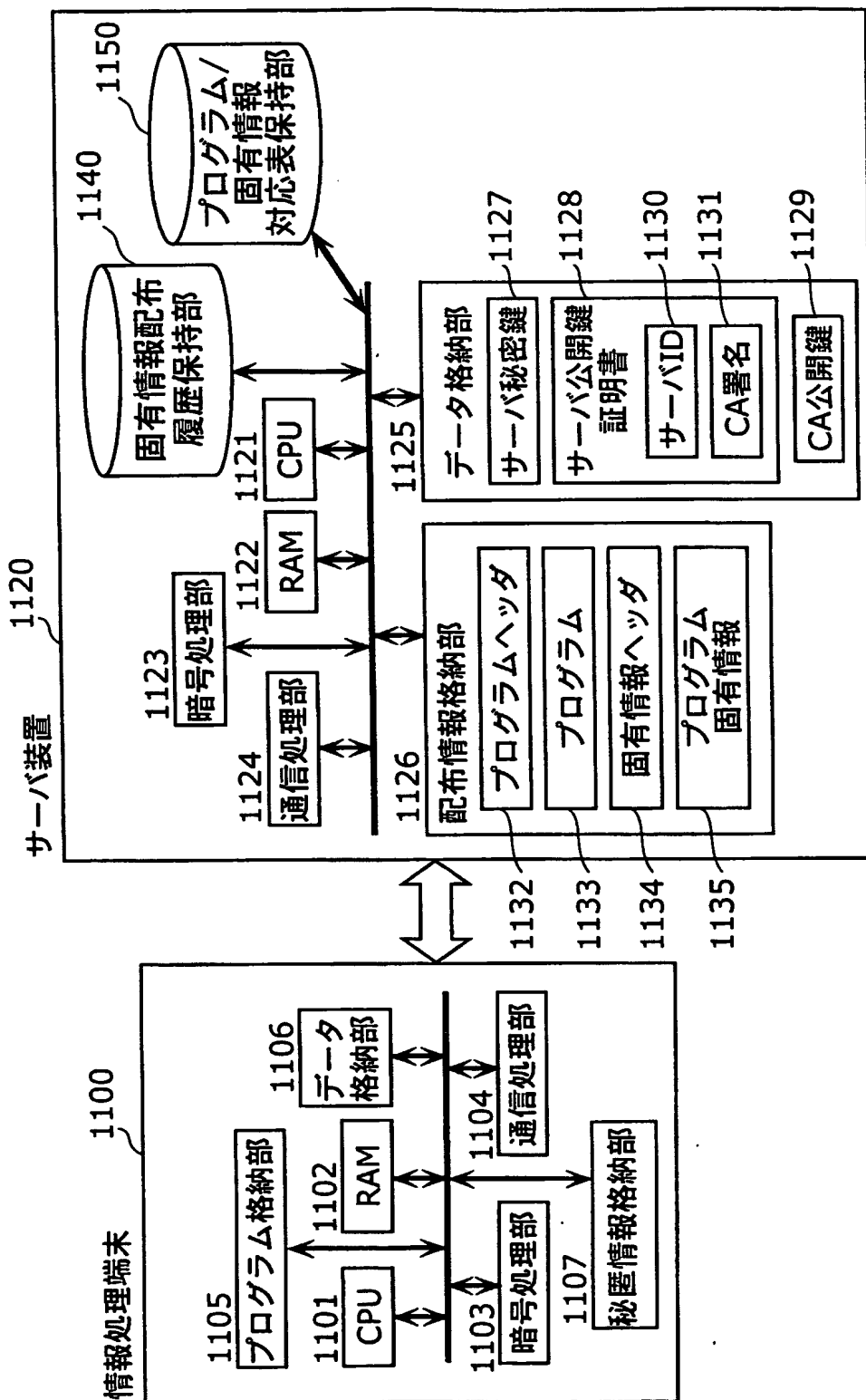


図12

(a)

固有情報配布履歴 1200

1201 端末ID	1202 プログラムID	1203 プログラム 固有情報ID	1204 最終配布日付
0001	0001	0001	2002.3.12
0002	0001	0002	2002.3.12
0010	0001	0003	2002.3.13
0015	0001	0004	2002.3.14
0020	0002	1001	2002.3.14

(b)

プログラム/固有情報対応表 1210

1211 プログラムID	1212 プログラム 固有情報ID	1213 配布開始ID
0001	0001~1000	0123
0002	1001~2000	1423
⋮	⋮	⋮

図13

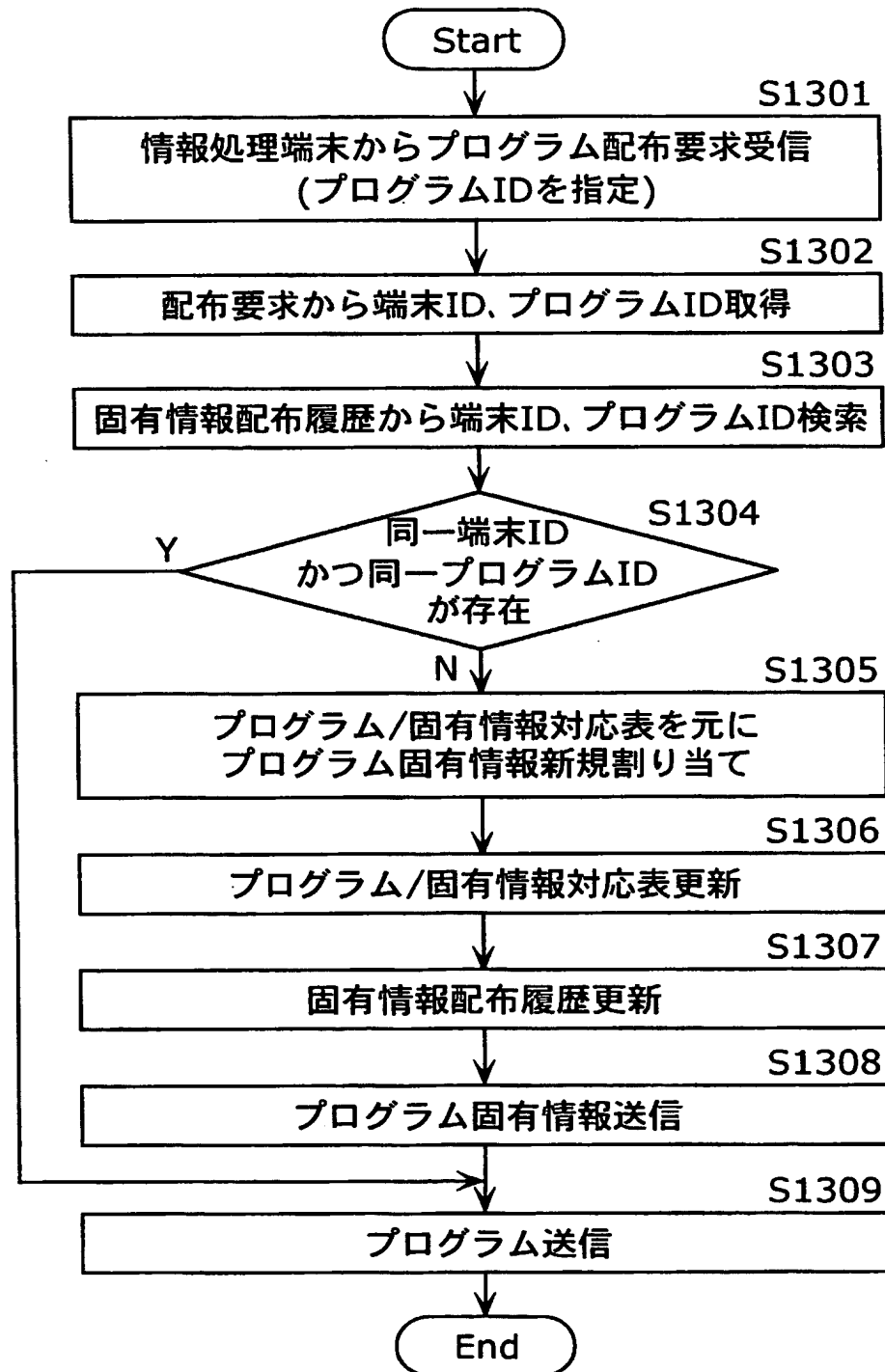


図14

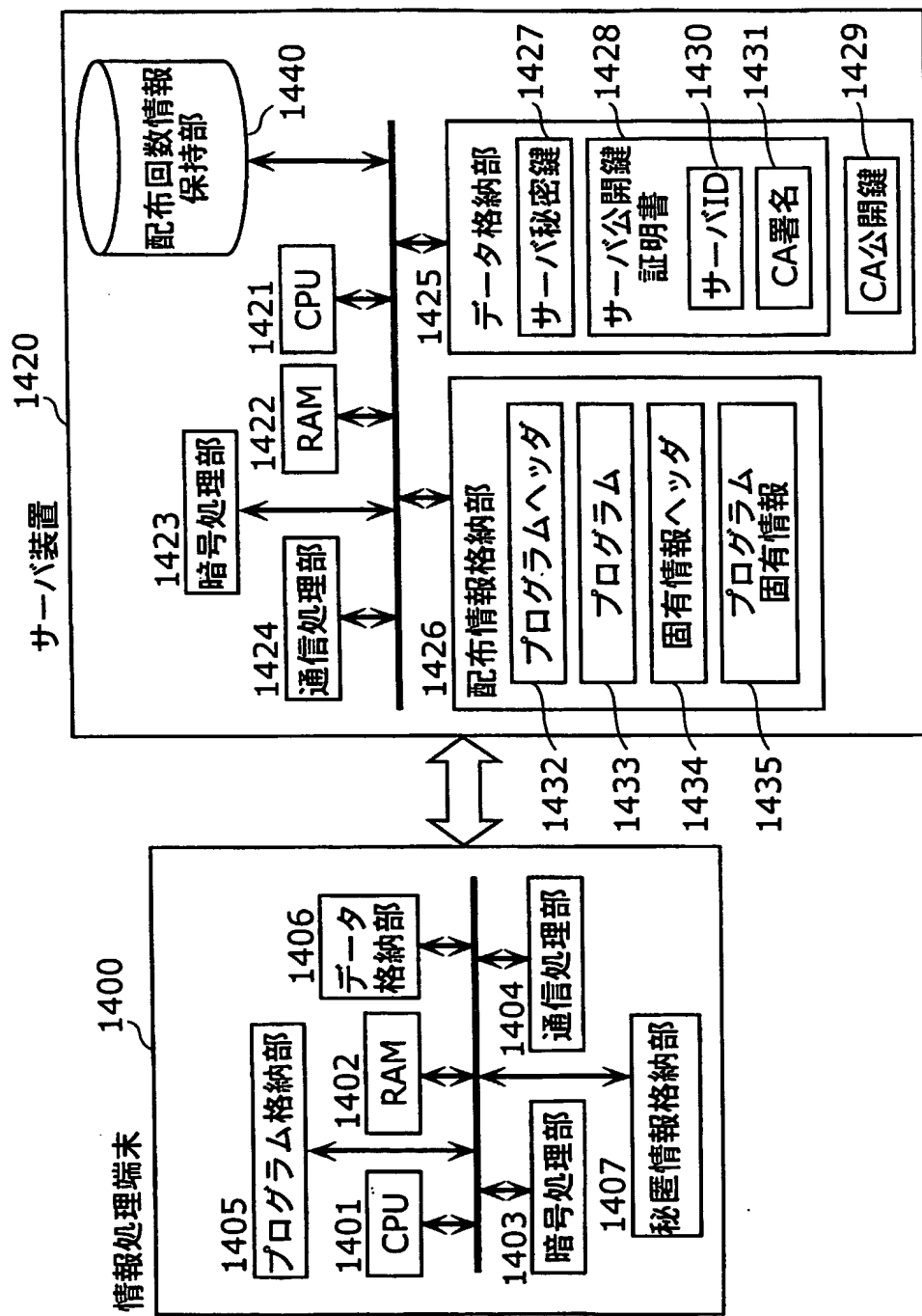


図15

配布回数情報

1500

1501 1502

端末ID	回数カウンタ
0001	1
0002	1
0003	0
⋮	⋮

図16

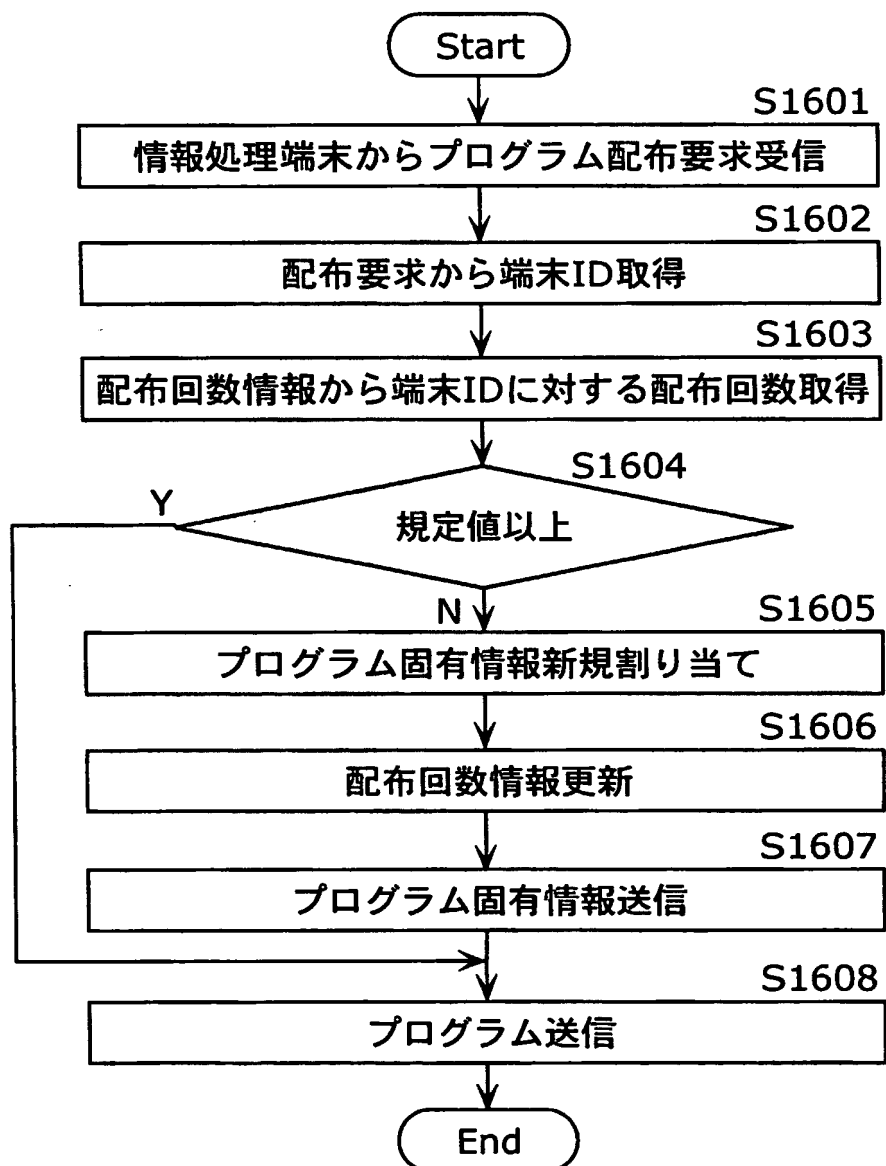


図17

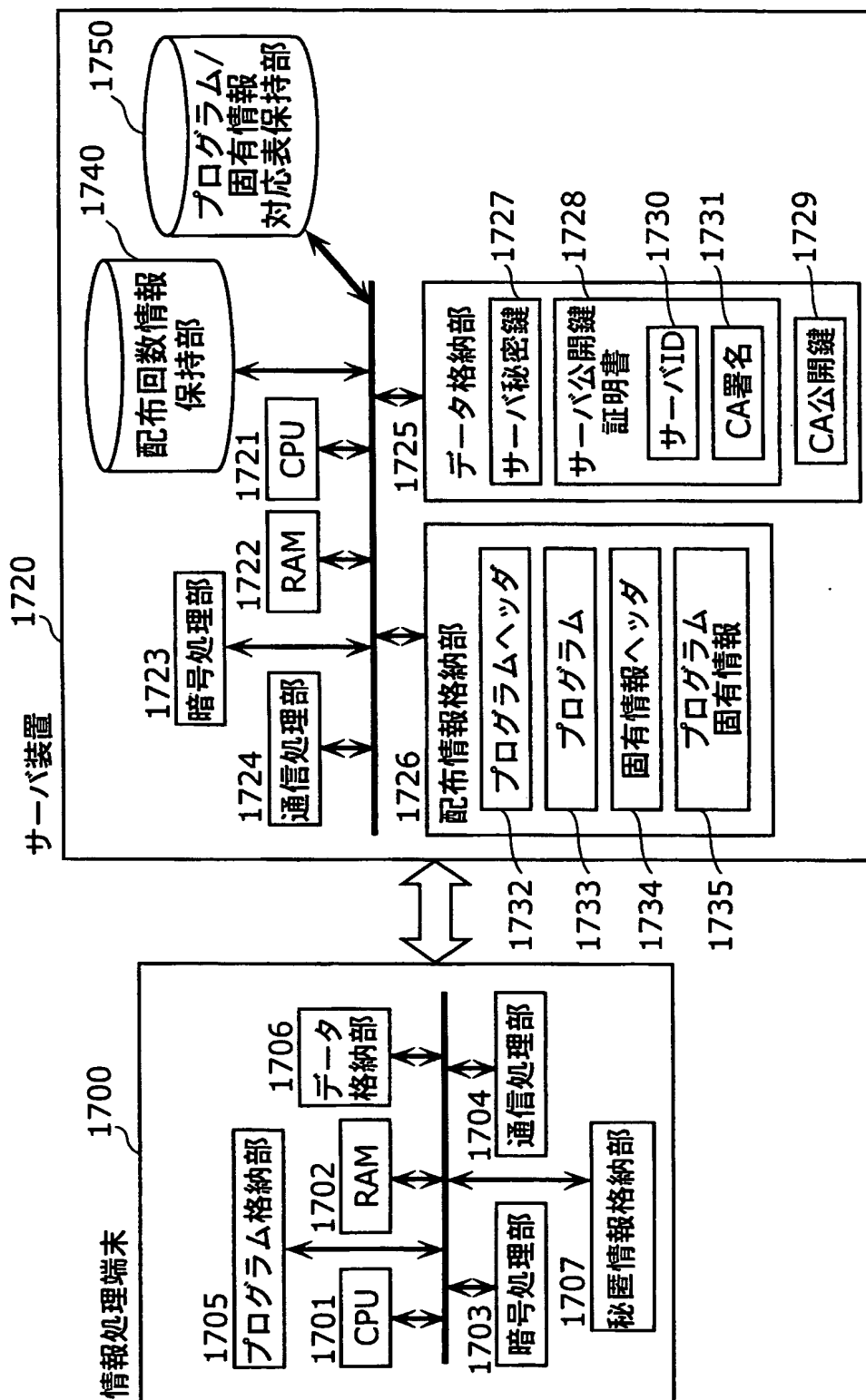


図18

(a)

配布回数情報 1800

1801 プログラムID	1802 端末ID	1803 回数カウンタ
0001	0001	1
0001	0002	1
0001	0003	0
0002	0001	1
0002	0002	0
0002	0003	0
⋮	⋮	⋮

(b)

プログラム/固有情報対応表 1810

1811 プログラムID	1812 プログラム 固有情報ID	1813 配布開始ID
0001	0001~1000	0123
0002	1001~2000	1423
⋮	⋮	⋮

図19

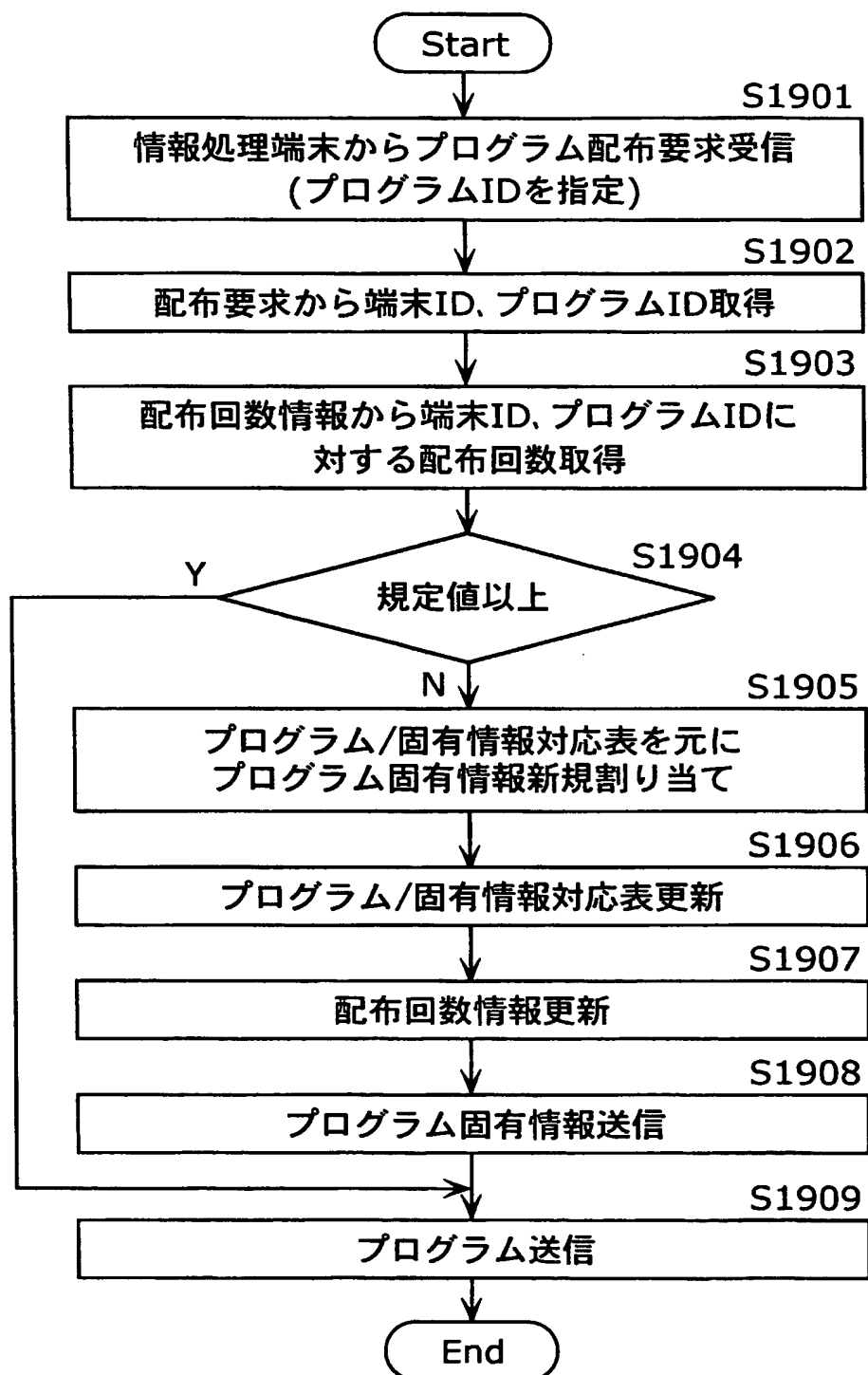


図20

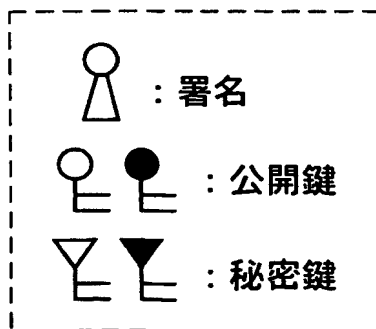
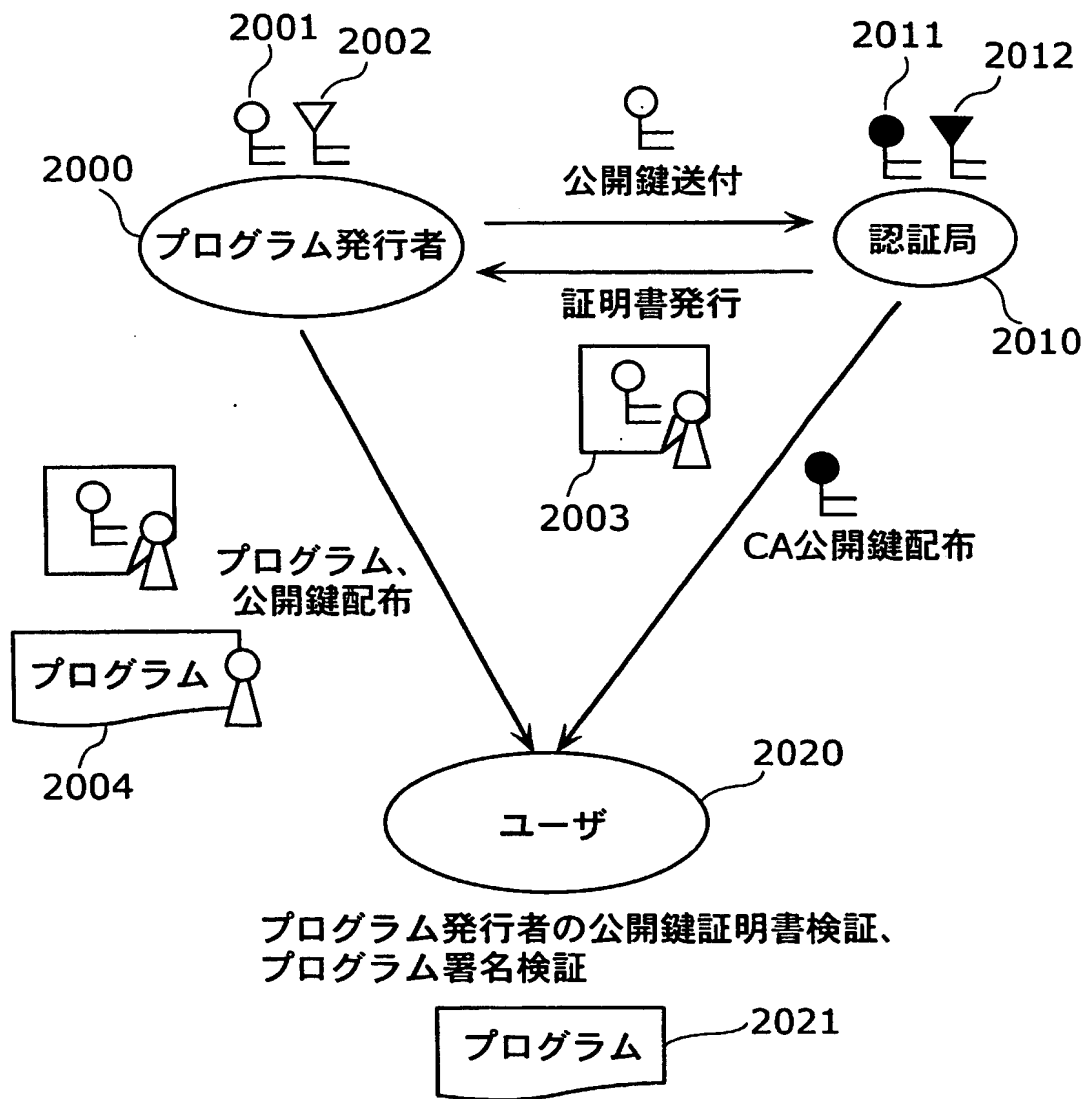
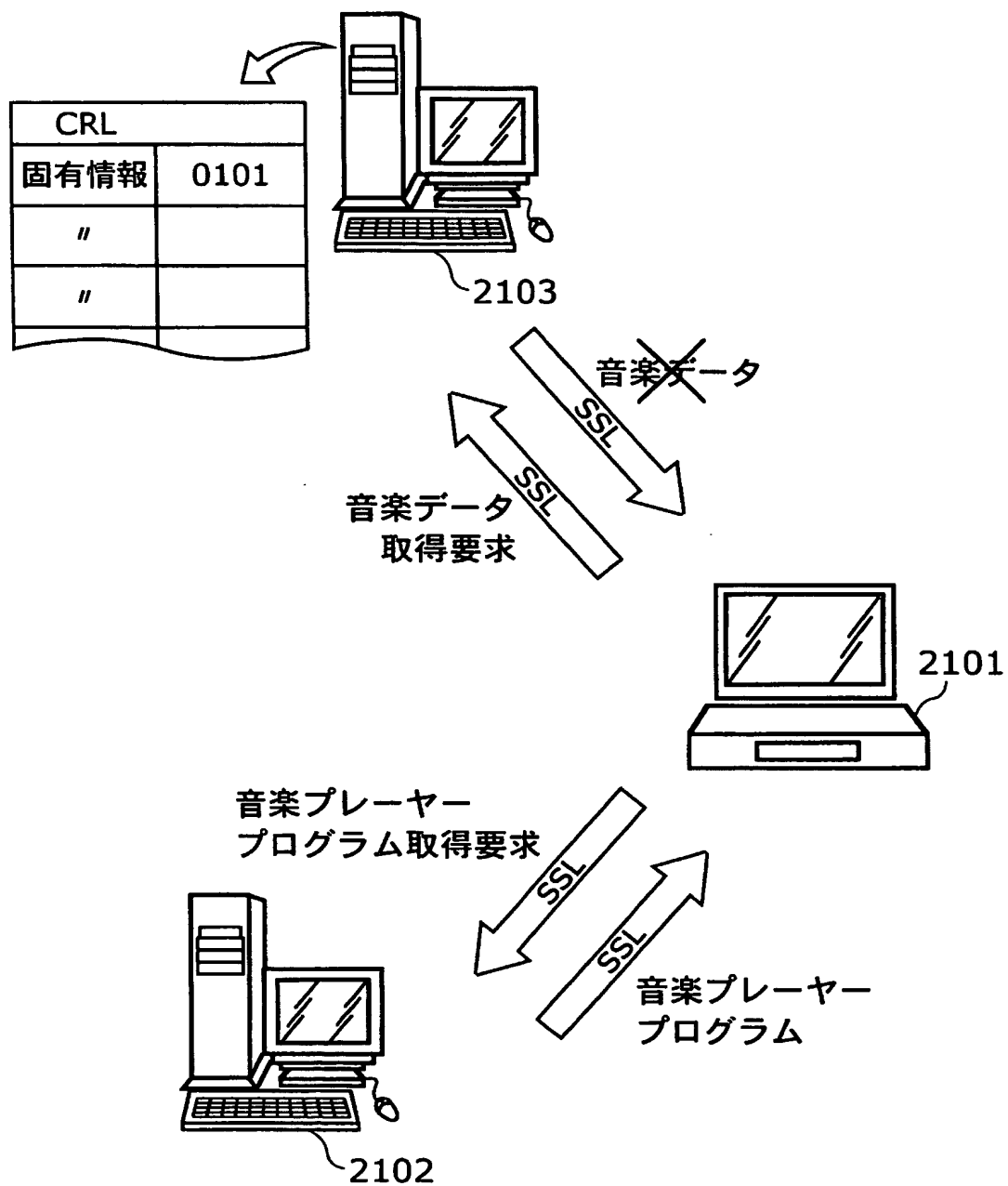


図21



INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/04808

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁷ G06F1/00, G06F9/445

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁷ G06F1/00, G06F9/445

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1926-1996 Jitsuyo Shinan Toroku Koho 1996-2003
Kokai Jitsuyo Shinan Koho 1971-2003 Toroku Jitsuyo Shinan Koho 1994-2003

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 8-190529 A (Fujitsu Ltd.), 23 July, 1996 (23.07.96),	1, 10, 11, 16, 17
Y	Full text; all drawings	7
A	(Family: none)	2-6, 8, 9, 12-15
Y	JP 2000-242491 A (Matsushita Electric Industrial Co., Ltd.), 08 August, 2000 (08.08.00), Full text; all drawings (Family: none)	7
A	JP 2002-91772 A (NEC Corp.), 29 March, 2002 (29.03.02), Full text; all drawings (Family: none)	1-17

☒ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:	"I" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document but published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search
29 July, 2003 (29.07.03)

Date of mailing of the international search report
12 August, 2003 (12.08.03)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP03/04808

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-311083 A (Casio Computer Co., Ltd.), 07 November, 2000 (07.11.00), Full text; all drawings (Family: none)	1-17

A. 発明の属する分野の分類 (国際特許分類 (IPC))

Int Cl⁷ G06F1/00, G06F9/445

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))

Int Cl⁷ G06F1/00, G06F9/445

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報 1926年-1996年

日本国公開実用新案公報 1971年-2003年

日本国実用新案登録公報 1996年-2003年

日本国登録実用新案公報 1994年-2003年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
X Y A	J P 8-190529 A (富士通株式会社) 1996. 07. 23, 全文, 全図 (ファミリーなし)	1, 10, 11, 16, 17 7 2-6, 8, 9, 12-15
Y	J P 2000-242491 A (松下電器産業株式会社) 2000. 08. 08, 全文, 全図 (ファミリーなし)	7

☒ C欄の続きにも文献が列挙されている。☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

29. 07. 03

国際調査報告の発送日

12.08.03

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

漆原 孝治

5B

9366

電話番号 03-3581-1101 内線 3546

C (続き) . 関連すると認められる文献		
引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP 2002-91772 A (日本電機株式会社) 2002. 03. 29, 全文, 全図 (ファミリーなし)	1-17
A	JP 2000-311083 A (カシオ計算機株式会社) 2000. 11. 07, 全文, 全図 (ファミリーなし)	1-17